Biblioteczka

Komputer Świat

Bezpieczny system Tails Live DVD/USB do anonimowego korzystania z internetu

+ zestaw najlepszych narzędzi do Windows do ochrony prywatności



JAK SKUTECZNIE ZAPEWNIĆ SOBIE

ANONIMOWOŚĆ W INTERNECIE

KOMPLETNY PORADNIK KROK PO KROKU

OMIJAJ BLOKADY I CENZURĘ!

NIE DAJ SIĘ SZPIEGOWAĆ!

Z TEJ KSIĄŻKI DOWIESZ SIĘ, JAK:

- chronić się przed szpiegowaniem
- zacierać wszelkie ślady
- szyfrować dyski, rozmowy, e-maile
- usuwać swoje dane z internetu
- ukrywać IP
- być zupełnie anonimowym w sieci

Z TĄ KSIĄŻKĄ E-WYDANIE GRATIS

Poniżej znajduje się płyta z kodem bonusowym dającym dostęp do e-wydania tej książki w serwisie KŚ+ (www.ksplus.pl) oraz do pliku ISO z obrazem załączonej płyty do pobrania.

PŁYTA 2 w 1

1. Jeśli wystartujemy z niej komputer, włączymy system Tails (patrz instrukcja na odwrocie koperty).

2. Jeżeli uruchomimy ją w Windows, uzyskamy dostęp do opisanych w książce programów zapewniających anonimowość i dbających o prywatność.

Jeśli brakuje płyty, poinformuj sprzedawcę lub redakcję: redakcja@komputerswiat.pl



Kod bonusowy należy zarejestrować w KŚ+ (ksplus.pl)

Biblioteczka Komputer Świat

KRZYSZTOF DZIEDZIC

JAK SKUTECZNIE ZAPEWNIĆ SOBIE

ANONIMOWOŚĆ W INTERNECIE

KOMPLETNY PORADNIK KROK PO KROKU

ringier
axel springer



AUTOR: Krzysztof Dziedzic

REDAKTORZY PROWADZĄCY: Rafał Kamiński, Agnieszka Al-Jawahiri

PRZYGOTOWANIE PŁYTY: Mariusz Michalski

PROJEKT OKŁADKI: Robert Dobrzyński

SKŁAD I ŁAMANIE: Robert Dobrzyński, Mariusz Rybak

KOREKTA: Jolanta Rososińska

WYDAWCA: RINGIER AXEL SPRINGER POLSKA Sp. z o.o.
02-672 Warszawa, ul. Domaniewska 52
tel. 22 2320000, 22 2320001
www.ringieraxelspringer.pl

ISBN: 978-83-8091-503-9

Warszawa 2018

DYREKTOR WYDAWNICZY: Paweł Paczuski

BUSINESS PROJECT MANAGER: Paweł Bulwan

DRUK I OPRAWA: Drukarnia im. Adama Półtawskiego, Kielce

EGZEMPLARZE ARCHIWALNE:
www.literia.pl

tel. 22 3367901
infolinia 801 000 869

E-WYDANIA: www.ksplus.pl

KONTAKT:
redakcja@komputerswiat.pl

INTERNET: komputerswiat.pl, ksplus.pl

ringier
axel springer





Krzysztof Dziedzic

od autora

Zachowanie prywatności podczas korzystania z internetu to jedno z największych wyzwań. Większość z nas nie może sobie pozwolić na to, żeby całkowicie zniknąć z sieci – korzystamy z serwisów społecznościowych i innego typu usług. Jednak należy zadać sobie pytanie: Czym powinniśmy dzielić się z całym światem, a co ma pozostać naszą tajemnicą?
W tej książce przedstawiłem wiele programów i porad, które pomogą Wam zachować anonimowość w sieci – to powinnien być dla każdego z nas priorytet. Zwłaszcza jeśli zależy nam na wolności słowa i obejściu cenzury. Pamiętajmy jednak o tym, że ponosimy odpowiedzialność za wykonywane w sieci akcje. Zapraszam do lektury!

1 Czego nie powinniśmy robić w sieci

PROGRAMY OPISANE W TYM ROZDZIALE ZNAJDZIESZ **NA DVD**

Z reguły to użytkownik komputera sam naraża swoją prywatność i bezpieczeństwo. Często nie zdajemy sobie sprawy z tego, co może być niebezpieczne. W pierwszym rozdziale książki poznamy najczęściej popełniane błędy, przez które przestajemy być anonimowi

Bezpieczeństwo i prywatność w sieci

W internecie jest dostępnych mnóstwo informacji na nasz temat, właściwie można stwierdzić, że jesteśmy śledzeni na każdym kroku.

Wszystkie odwiedzane przez nas strony, wyszukiwane słowa, przesyłane wiadomości, hasła, loginy – te i znacznie więcej informacji można **przechwycić w ruchu sieciowym**. Wiele informacji na nasz temat trafia także **na serwery naszego dostawcy internetu**. Wszystko to stwarza duże zagrożenie, gdyż uzyskane o nas informacje mogą być użyte na naszą niekorzyść.

Prywatności zagrażają również duże firmy, które potrzebują danych dotyczących naszych internetowych zwyczajów, by przygotować specjalny **profil użytkownika i na jego podstawie móc wyświetlać nam reklamy** (są to tak zwane reklamy behawioralne). Teoretycznie korzystamy z wielu usług za darmo, choćby z Google, ale w praktyce wiąże się to z **przekazywaniem naszych danych różnym firmom**.

Korzystając z **serwisów społecznościowych**, sami zgadzamy się na pokazywanie naszego prywatnego życia publicznie. Oczywiście, należy konfigurować opcje prywatności, jednak trzeba też pamiętać, że każda informacja, którą umieszczamy w takim serwisie i udostępniamy innym, ma zasięg globalny i może zostać wykorzystana. Aktywne korzystanie z serwisów społecznościowych jest zupełną przeciwnością prywatności i bezpieczeństwa w sieci.

Jeśli zależy nam na prywatności, powinniśmy zastosować się do porad i rozwiązań przedstawionych w tej książce. Dowiemy się z niej, których programów i usług internetowych używać, by pozostać anonimowym w sieci. Nauczymy się zacierać ślady, jakie pozostawiamy, korzystając z komputera, oraz takie, które zostawiamy w internecie – przeczytamy nawet, jak zniknąć z sieci. Poznamy też praktyczne porady, w jaki sposób korzystać bezpiecznie z usług internetowych i jak bez narażania prywatności, ale swobodnie, używać internetu.

7 najczęstszych błędów zdradzających naszą tożsamość

Na kolejnych stronach tej książki poznamy rozwiązania, które umożliwią nam pozostanie anonimowym w internecie, wiele z nich dotyczyć będzie korzystania ze specjalnej sieci i przeglądarki Tor, która ukrywa nasz prawdziwy adres IP. Musimy jednak pamiętać, że będzie można nas wykryć, jeśli będziemy popełniać podstawowe błędy w trakcie korzystania z takiej sieci.

1 Nie logujemy się do wcześniej założonych kont z sieci Tor

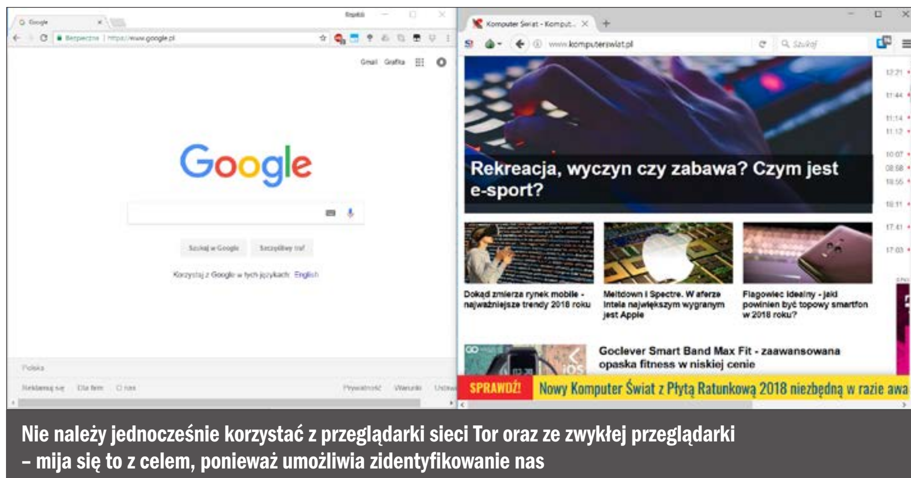
Jest to absolutnie zabronione. Z założenia każde konto zabezpieczone jest hasłem i wszystkie informacje dotyczące logowania zapisywane są na serwerze. Jeśli więc zalogujemy się na nasze konto, korzystając z sieci Tor, będzie można powiązać nasz nowy adres IP z nami jako użytkownikiem konta. Zyskamy tylko poczucie fałszywego bezpieczeństwa. **O sieci Tor przeczytamy w rozdziale szóstym.**

2 Nie logujemy się na konta z dostępem do pieniędzy przez sieć Tor

Tego typu konta są ogólnie jawne dla usługodawców, którzy świadczą nam daną usługę. Musimy być odpowiednio zweryfikowani, zanim otworzymy rachunek bankowy czy też potwierdzimy konto PayPal. Dlatego też nie ma sensu ukrywać swojej obecności w internecie i logować się do tego typu usług, korzystając z Tora. Możemy również przysporzyć sobie kłopotów, ponieważ banki w ramach zabezpieczenia mogą blokować konta, do których następują logowania z różnych adresów IP w różnych krajach.

3 Nie zmieniamy typu wykorzystywanej sieci w trakcie trwania jednej sesji

Jeśli korzystamy z sieci Tor przez na przykład 30 minut i stwierdzimy, że pracuje ona zbyt wolno, a chcemy obejrzeć jakiś materiał, choćby film, szybciej, nie otwieramy zwykłej przeglądarki i nie przeglądamy zasobów przy jednocześnie aktywnej przeglądarce Tor. Przez takie działanie bardzo łatwo powiązać adresy IP i czasy dostępu do serwerów. Powinniśmy całkowicie zamknąć przeglądarkę Tor i dopiero wtedy korzystać normalnie z internetu.



Nie należy jednocześnie korzystać z przeglądarki sieci Tor oraz ze zwykłej przeglądarki – mija się to z celem, ponieważ umożliwia zidentyfikowanie nas

4 Nie przesyłamy wrażliwych danych bez ich zaszyfrowania

Nie wiemy, kto może nas szpiegować, być może nikt, a być może jakaś zorganizowana grupa. Faktem jednak jest, że wszelkiego rodzaju informacje, które są wrażliwe lub szczególnie ważne, nigdy nie powinny być przesyłane przez internet bez wcześniejszego zaszyfrowania. Jeśli nie zamierzamy korzystać ze specjalnych narzędzi do szyfrowania, powinniśmy przynajmniej spakować przesyłane pliki do archiwum i zabezpieczyć je hasłem. Nie jest to idealne rozwiązanie, ale szybkie, a jeśli ustawimy odpowiednio silne hasło, będzie ono nie do złamania dla zwykłych atakujących.

Szyfrowanie
Wprowadź hasło:
****
Wprowadź ponownie hasło:
****
Pokaż hasło
Metoda szyfrowania: AES-256

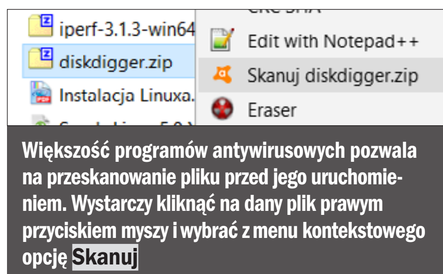
Jeśli korzystamy z programu 7-Zip, wybierzmy metodę szyfrowania AES-256, która zapewnia wysoki poziom bezpieczeństwa

SZYFROWANIE

Do przesyłania szyfrowanych wiadomości e-mail warto wykorzystywać program Thunderbird wraz z dodatkiem Enigmail. Jeśli chcemy zabezpieczyć komunikację na urządzeniach mobilnych, powinniśmy zacząć korzystać z aplikacji Signal. Opis konfiguracji tych narzędzi znajdziemy w rozdziale szóstym.

5 Nie otwieramy nieznanych linków i plików

Otrzymany na przykład w e-mailu link może otwierać prawdziwą stronę internetową, ale może też być to pułapka prowadząca do zainfekowanej witryny, która wykorzystując specjalne skrypty, przechwyci naszą przeglądarkę lub zainstaluje programy typu malware. Podobne zagrożenie zawsze istnieje, gdy otwieramy nieznane pliki, które otrzymaliśmy drogą mailową lub sami pobraliśmy z podejrzanych stron. Wirusy mogą być ukryte nie tylko w aplikacjach, ale również w plikach muzycznych, zdjęciach, dokumentach. Jeśli zależy nam na ochronie, powinniśmy zainstalować program antywirusowy, który ochroni nas przed tego typu zagrożeniami jeśli już przypadkiem otworzyliśmy zły link.



Większość programów antywirusowych pozwala na przeskanowanie pliku przed jego uruchomieniem. Wystarczy kliknąć na dany plik prawym przyciskiem myszy i wybrać z menu kontekstowego opcję **Skanuj**

6 Nie podajemy informacji na nasz temat online

Jeśli zależy nam na anonimowości, nie możemy na stronach internetowych podawać dotyczących nas informacji. Takie dane, jak wiek, data urodzenia, miejsce zamieszkania, ulubione zwierzę, drużyna czy zespół, przezwisko, hobby i inne tego typu – z pozoru wydają się mało szkodliwe. Jednak na przykład często, gdy chcemy odzyskać hasło do jakiejś usługi, musimy podać właśnie takie informacje. Jeśli więc opublikujemy je w serwisie społecznościowym lub innym publicznym portalu, atakujący mogą do nich dotrzeć i je wykorzystać.

7 Nie stosujemy słabych haseł

Informacje osobiste mogą także wykorzystywać generatory do łamania haseł. Wystarczy znać kilka podstawowych danych i już można złamać hasło większości mniej doświadczonych użytkowników. Bardzo dużo osób używa jako hasła na przykład swojego imienia i roku urodzenia lub nazwy drużyny piłkarskiej itp. Pamiętajmy, że musimy zabezpieczać nasze konta silnymi hasłami, które nie będą podatne na tego typu „społecznościowe" ataki. Silne hasło powinno mieć przynajmniej 12 znaków, na które składać się będzie przynajmniej jedna duża litera, cyfra i znak specjalny. Możemy skorzystać ze specjalnych generatorów haseł, na przykład **https://generator.blulink.pl/**

Ustawienia
Ile znaków? 12
Ile haseł? 25
Hasło zawiera:
☑ małe litery: [a b c...]
☑ wielkie litery: [A B C...]
☑ cyfry: [1 2 3...]
☐ znaki interpunkcyjne: [: ! ?...]
☑ znaki specjalne: [@ # $...]
☑ bez znaków podobnych: [i l O 1 0 I]
Dodatkowe ustawienia
Muszą wystąpić znaki:
Mogą wystąpić znaki:
Nie mogą wystąpić znaki:
Generuj

TdBt/57a<Z*x
XmAUAE8\2$Uc
TbH/p9NGL3AV
\k/HJBFkzTE>
cqKCtjtMTAVG
oo3>Qf82Zhoo
w*7wYq/BeTR8
CJy9XUuLGWXa
C/Bfr#3o+>j7
#smgLCP2ZMA@
k=M^5oemwuZn
v*a$FSaHKV#9
cRABgNC2W36^
PKqLDQ<>WmCf
Cq#ZL%>@UMCA
eSeAyJEN8-cp
Xo@y8Cep*fPS
j2TCsaR6*/k%
T$R%<+s9ut83
/LRC%k9nL^$C
eTnk37pzaE$m
MvUGp^oxQDAT
@nFMsH37fPQG
yEG8XKToEr++
vu^K<Eh>^@Yw

Wprowadzamy parametry i klikamy na **Generuj** – po chwili w oknie po prawej pojawią się losowe hasła. Możemy wybrać jedno z nich i z niego korzystać

TYMCZASOWE ADRESY E-MAIL

Jeśli chcemy założyć konto w jakimś serwisie, żeby uzyskać dostęp do plików lub treści, która nas interesuje, i w tym celu musimy podać e-mail – dobrym rozwiązaniem jest skorzystanie z adresu tymczasowego. Tego typu adresy można tworzyć bardzo szybko za pomocą stron internetowych, takich jak na przykład **https://pl.getairmail.com**. Dzięki takiemu rozwiązaniu nie będziemy zaśmiecać naszej głównej skrzynki e-mail.

Wchodzimy na stronę **https://pl.getairmail.com** i klikamy na **Wygeneruj adres e-mail**. Od razu otworzy się okno z naszą nową skrzynką. Adres będzie losowy – wystarczy go podać przy rejestracji. Skrzynka odświeżana jest automatycznie, więc będziemy mieli dostęp do przychodzących wiadomości. Skrzynka jest aktywna tak długo, dopóki jest otwarta na karcie przeglądarki. Po zamknięciu karty zostanie skasowana po 24 godzinach.

2 Programy do ochrony prywatności

PROGRAMY OPISANE W TYM ROZDZIALE ZNAJDZIESZ NA DVD

W tym rozdziale poznamy najlepsze narzędzia, programy i usługi, z których można korzystać w systemie Windows do ochrony naszej prywatności. Dowiemy się także, jakie firmy nas szpiegują i udostępniają dotyczące nas dane

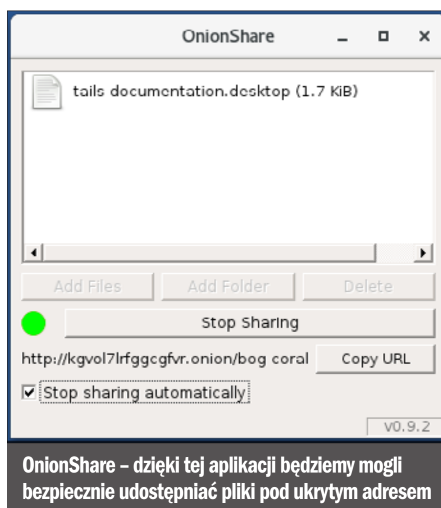
Narzędzia polecane przez Edwarda Snowdena

Edward Snowden – demaskator, który ujawnił informacje na temat inwigilacji przeprowadzanej przez rząd USA – był ścigany listem gończym i okrzyknięty wrogiem publicznym, a jednak udawało mu się bezpiecznie umieszczać treści w internecie tak, by nie zostać wyśledzonym. Do tego celu wykorzystywał specjalne narzędzia i programy. Co ciekawe, większość z tych aplikacji jest prosta w użyciu i każdy może je stosować, gdyż są darmowe i oparte na otwartym kodzie. Wszystkie znajdziemy na dołączonej do książki płycie.

Tor

Jest to sieć anonimizująca, która nie ma sobie równych pod względem skuteczności. Opiera się na niej wiele narzędzi, które ukryją naszą tożsamość w internecie, między innymi: **Tor Browser** – przeglądarka z wieloma dodatkami, **SecureDrop** zapewniający możliwość anonimowego zamieszczania treści (korzystają z tego rozwiązania duże organizacje medialne), **OnionShare**, który pozwala na anonimową wymianę plików.

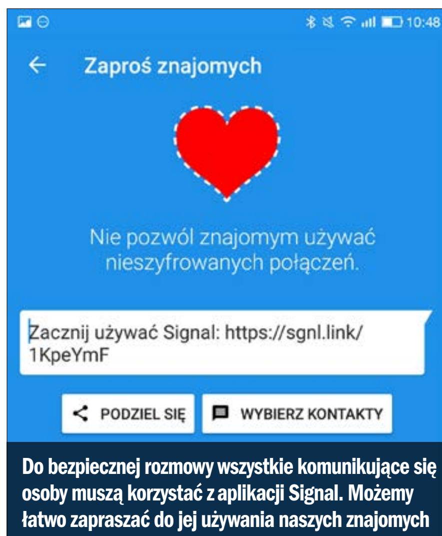
Zastosowań sieci Tor jest naprawdę dużo. W jednym z ujawnionych przez Snowdena dokumentów możemy przeczytać, że NSA (amerykańska agencja bezpieczeństwa), stwierdza, że Tor jest najlepszą siecią tego typu i nie ma żadnych konkurentów.



OnionShare – dzięki tej aplikacji będziemy mogli bezpiecznie udostępniać pliki pod ukrytym adresem

Signal

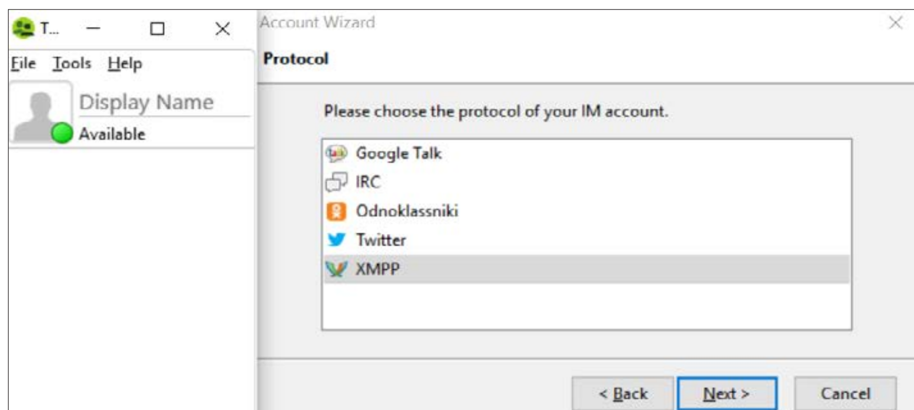
Snowden korzystał bezpiecznie także ze smartfonów. Oprócz specjalnej wersji systemu Android do komunikacji wykorzystywał program **Signal**, który działa na Androidzie i na iOS. Ta aplikacja funkcjonuje podobnie do wszystkich komunikatorów, jednak zapewnia szyfrowane połączenie pomiędzy dwoma stronami uczestniczącymi w rozmowie. Treść rozmowy jest niemożliwa do odtworzenia dla osób trzecich. Możemy również wysyłać wiadomości, gdy nasz odbiorca jest offline. Co ciekawe, możliwa jest także grupowa rozmowa z zachowaniem całkowitego bezpieczeństwa. W sklepie Google Play znajdziemy tę aplikację pod nazwą **Signal Private Messenger**.



Do bezpiecznej rozmowy wszystkie komunikujące się osoby muszą korzystać z aplikacji Signal. Możemy łatwo zapraszać do jej używania naszych znajomych

OTR

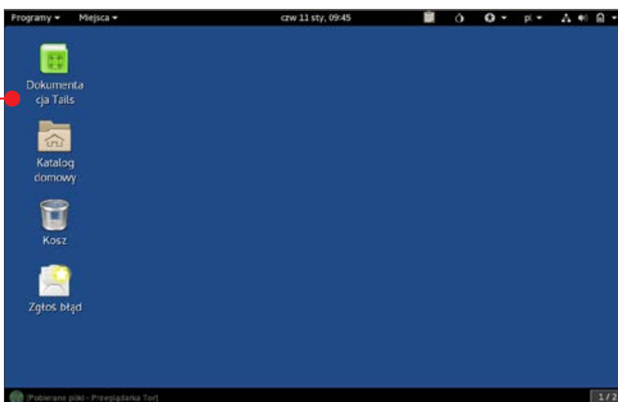
OTR to skrót od **Off-The-Record**, co w tłumaczeniu oznacza „nieoficjalny".
Jest to protokół szyfrujący, który według danych dostarczonych przez Snowdena sprawia problemy największym agencjom bezpieczeństwa, gdyż jest „nie do złamania", jak wynika z ich raportów. Został zaprojektowany jako modularny kod, który może być łatwo zaimplementowany jako wtyczka do różnego typu programów. W większości przypadków jest to bardzo dobre rozwiązanie, nie sprawdza się tylko w przypadku aplikacji, które mają inne błędy sprawiające, że są podatne na ataki.
Najbezpieczniejsze aplikacje korzystające z protokołu OTR to **ChatSecure**, dostępny na urządzenia mobilne, i **Tor Messenger** – na komputery.
Ciekawą alternatywą jest również **Pidgin**, domyślnie dostępny komunikator w wielu dystrybucjach systemu Linux, który wymaga zainstalowania wtyczki z OTR.



Tor Messenger – nie tylko korzysta z sieci Tor, która ukrywa naszą tożsamość, ale też wykorzystuje protokół szyfrujący OTR, dzięki czemu nasze rozmowy są całkowicie bezpieczne

TAILS

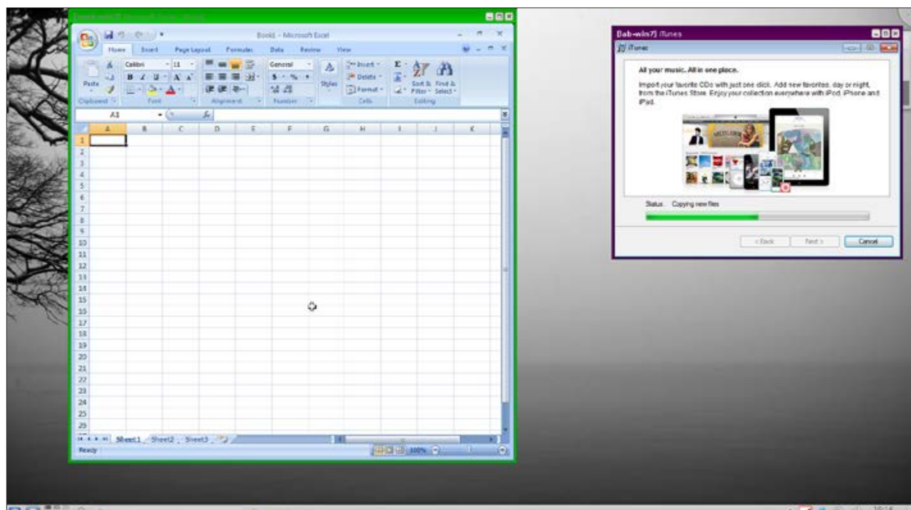
Specjalny system operacyjny oparty na dystrybucji Debian – to jeden z najbezpieczniejszych systemów Linux. Jest przeznaczony zarówno dla początkujących, jak i dla zaawansowanych użytkowników. Więcej na jego temat przeczytamy w rozdziale siódmym, który jest mu poświęcony w całości. Tails był wielokrotnie opisywany przez Snowdena jako system, który zapewnił mu możliwość anonimowego udostępnienia wielu ważnych dokumentów.



Qubes OS

Kolejny system operacyjny, który służy do zachowania anonimowości i zapewnienia bezpieczeństwa użytkownikom. Jest on bardzo oryginalny, opiera się bowiem na wirtualnych maszynach. Właściwie zawsze, gdy chcemy skorzystać z jakiejś aplikacji czy otworzyć podejrzany plik, możemy zrobić to w nowo utworzonej „w locie" maszynie wirtualnej. Zapewnia to niebywały poziom bezpieczeństwa. Oprócz tego możemy dowolnie korzystać z przestrzeni dyskowej, ponieważ nie jest to system w wersji Live. Jest to dość skomplikowany system, przeznaczony raczej dla bardziej doświadczonych użytkowników.

Rozwiązanie dla ambitnych: możemy uruchomić system Tails wewnątrz Qubes OS dla zachowania jeszcze większej anonimowości.



Każda aplikacja może być otworzona w nowej wirtualnej maszynie – zapewnia to niezwykle wysoki poziom bezpieczeństwa, jednak wymaga dość mocnego komputera

PROGRAM PRISM

To od ujawnienia przez Snowdena PRISM, tajnego amerykańskiego programu szpiegowskiego, rozpoczęły się wysiłki wielu twórców i deweloperów, by zapewnić sobie możliwie jak największą prywatność. W skrócie: program jest aktywny od 2007 roku i umożliwia NSA dostęp do serwerów największych przedsiębiorstw internetowych, jak również gromadzenie ich danych na własny użytek. Oznacza to, że inwigilacji podlegają wszyscy, którzy korzystają z usług takich firm, jak Google, Microsoft, Facebook, Apple i inne. Z ujawnionych dokumentów wynika, że firmy te zgodziły się na działanie tego programu i nie odbywa się to wbrew ich woli. Udostępniane NSA dane dotyczą między innymi wszystkich wiadomości pocztowych, zasobów dysków internetowych, wszystkich zdjęć i filmów, danych przekazywanych jako transfer plików, danych z komunikatorów tekstowych i wideo, danych z serwisów społecznościowych, jak również loginów. Informacje ujawnione przez Snowdena zostały potwierdzone przez dyrektora centrali wywiadu. Zagrożenie prywatności jest ogromne, gdyż program PRISM obejmuje oficjalnie dane przepływające przez serwery w USA, co oznacza, że mogą być inwigilowani użytkownicy z całego świata. Rozwiązaniem tego problemu może być stosowanie bezpiecznych programów, które zapewniają anonimowość i szyfrowane, bezpieczne kanały komunikacji.

Rozwiązania dla osób, które chcą korzystać z systemu Windows

Można powiedzieć, że jeśli Microsoft przystąpił do programu PRISM, to jego system nie zapewnia anonimowości. Tymczasem standardowo, jako zwykli użytkownicy, oczekujemy po prostu prywatności naszych wiadomości, plików itp. Nie musimy zachowywać się tak, jakbyśmy byli ścigani międzynarodowym listem gończym. Warto jednak korzystać z programów, które pozwalają na szyfrowaną komunikację czy też wymianę plików, ponieważ ochroni nas to przed osobami trzecimi, które będą chciały wykorzystać uzyskane dane w szkodliwy dla nas sposób. Jeśli często używamy publicznych, otwartych sieci bezprzewodowych, nie wiemy, czy ktoś nie skanuje ruchu sieciowego i nie czeka na to, by przechwycić nasz login i hasło lub wiadomości, które przesyłamy.

Dlatego trzeba w systemie Windows zadbać o naszą ochronę przed tego typu atakami.

Szpiegowanie i telemetria w Windows

System Windows domyślnie ma włączonych wiele funkcji, które w gruncie rzeczy służą tworzeniu profilu użytkownika, który później może być wykorzystany do tego, by na jego podstawie mogły nam być przedstawiane spersonalizowane reklamy. Na serwery Microsoftu przesyłane są również dane dotyczące naszego sprzętu czy wykonywanych przez nas operacji itp.

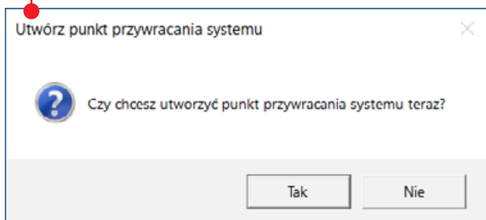
Warto więc zainstalować specjalny program, który pomoże nam wyłączyć wszystkie te zupełnie zbędne z punktu widzenia użytkownika funkcje, które zużywają transfer i moc obliczeniową naszego komputera po to, by nas śledzić.

W tej roli sprawdzą się programy **Ashampoo AntiSpy** lub **O&O Shutup 10**. Przyjrzyjmy się bliżej temu pierwszemu.

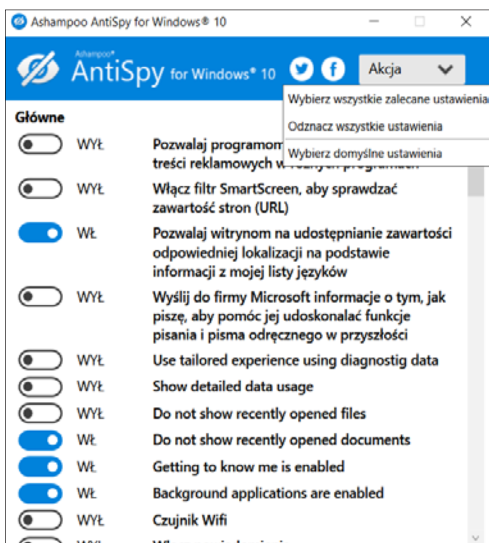
Wyłączanie szpiegowania

■ Ashampoo AntiSpy

1 Po uruchomieniu programu pojawi się informacja dotycząca utworzenia punktu przywracania systemu. Punkt przywracania przyda się na wszelki wypadek – gdyby coś poszło nie tak, będziemy mogli cofnąć zmiany. Klikamy na **Tak**.



2 Klikamy w górnym prawym rogu okna na **Akcja**, **Wybierz wszystkie zalecane ustawienia**, a gdy pojawi się ostrzeżenie, potwierdzamy je, klikając na **Tak**.



3 Jeśli chcemy, możemy także sami decydować o każdej opcji, włączając lub wyłaczając każdą z osobna.

4 Aby zastosować zmiany, musimy ponownie uruchomić komputer.

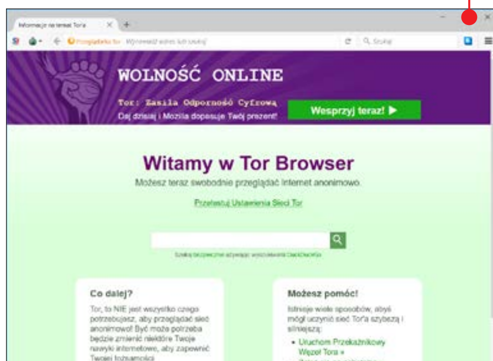
Najlepsze programy chroniące przed PRISM

Poznajmy teraz najważniejsze programy dla systemu Windows, które ochronią nas przed programem PRISM oraz przed praktycznie każdym atakiem na naszą prywatność przez osoby trzecie. Niektóre z nich będą szerzej omawiane w dalszej części książki wraz z odpowiednimi poradami. Wszystko to są programy i usługi, z których każdy z nas może korzystać.

Przeglądarka

■ Tor Browser

To najlepszy wybór dla użytkowników Windows ze względu na komunikację przeprowadzoną poprzez specjalną sieć Tor. Należy korzystać z tej przeglądarki tylko wtedy, gdy naprawdę tego potrzebujemy. Do normalnych zastosowań może wydać nam się zbyt wolna, gdyż transfer w dużej mierze zależy od tego, jaki obwód zostanie nam przyznany. Opis korzystania i działania tej przeglądarki oraz jej dodatków znajdziemy w rozdziale szóstym.



Bezpieczna chmura

■ Kolab NOW

Trudno stwierdzić, czy jakakolwiek usługa oferująca przechowywanie danych na serwerach zewnętrznych jest bezpieczna. Jedną z nielicznych polecanych jest Kolab NOW. Jest to serwis, który oferuje przechowywanie naszych danych w Szwajcarii, gdzie



prawo nie pozwala na inwigilację plików umieszczonych na serwerach. Niestety, jest to usługa płatna i kosztuje około 10 franków szwajcarskich na miesiąc. W zamian otrzymujemy 2 GB miejsca i konto pocztowe, również z gwarancją anonimowości. Nie jest to idealne rozwiązanie – jeśli mamy możliwość, lepiej samemu postawić serwer, który będzie naszą chmurą. Wymaga to jednak wiedzy technicznej i wstępnej inwestycji. Adres usługi: **https://kolabnow.com**

Serwisy e-mail

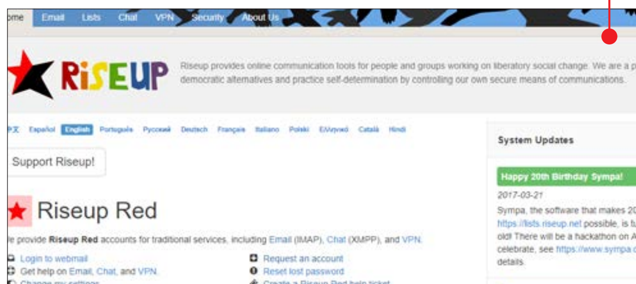
Używanie serwerów pocztowych dużych korporacji oznacza brak anonimowości. Dane z serwerów mogą być odczytane przez agencje bezpieczeństwa i nie mamy możliwości zabezpieczenia się przed tym. Najlepiej jest korzystać z usług firm, które zapewniają anonimowe konta pocztowe – wtedy nasze dane będą zawsze bezpieczne i tylko my będziemy mieli do nich dostęp. Oto dwie takie usługi, które są warte uwagi.

Autistici/Inventati

Serwis jest dostępny za darmo – jednak nie tak łatwo uzyskać do niego dostęp. Musimy na stronie **https://www.autistici.org/u/services** kliknąć na **Start request**. Następnie podajemy wszystkie dane potrzebne do rejestracji. Kolejnym etapem jest napisanie w języku angielskim specjalnej informacji o sobie, dotyczącej tego, dlaczego chcemy skorzystać z tej usługi. Taki wpis zostanie później sprawdzony przez administratora i dopiero, gdy on wyrazi zgodę, zostanie nam przyznane konto pocztowe. Chodzi tu głównie o odróżnienie botów od ludzi, więc jeśli napiszemy chociaż kilka sensownych linijek, nie powinno być problemu z utworzeniem konta.

Riseup

To darmowy serwis (**https://riseup.net**), który pozwoli nam na korzystanie z usług e-mail, a dodatkowo z czatu oraz klienta VPN. Jest to bardzo atrakcyjna oferta, jednak ma spore ograniczenie, jeżeli chodzi o możliwości rejestracji



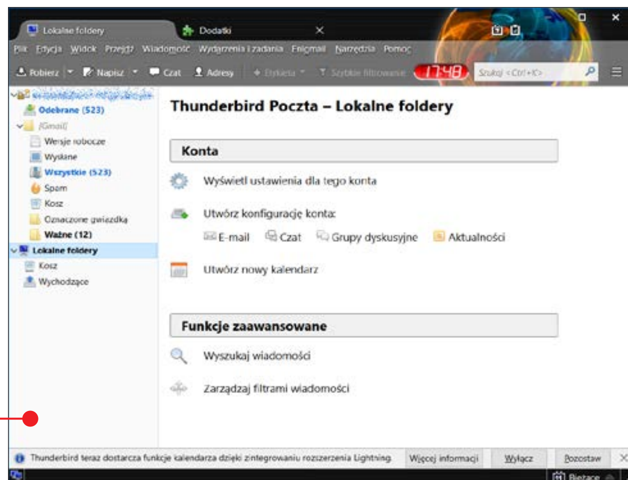
nowych kont. Wymagane są specjalne kody zaproszeniowe, które można uzyskać tylko i wyłącznie od aktywnych użytkowników. Dzięki temu usługa nie jest wykorzystywana przez spamerów i boty. Możemy spróbować uzyskać taki kod, pisząc w języku angielskim wiadomość na adres pomocy Riseup (w uzyskaniu kodu mogą być też pomocne społeczności serwisów Wykop i Reddit).

A/I New Service Request

Start request

Klient poczty e-mail

Oprócz bezpiecznego konta e-mail będziemy potrzebować bezpiecznego klienta poczty. Zdecydowanie należy wybrać takiego, który jest oparty na otwartym oprogramowaniu, ponieważ jeżeli oprogramowanie jest czyjąś własnością i jest zamknięte, rodzi to wątpliwości co do sposobu przechowywania i bezpieczeństwa wiadomości.

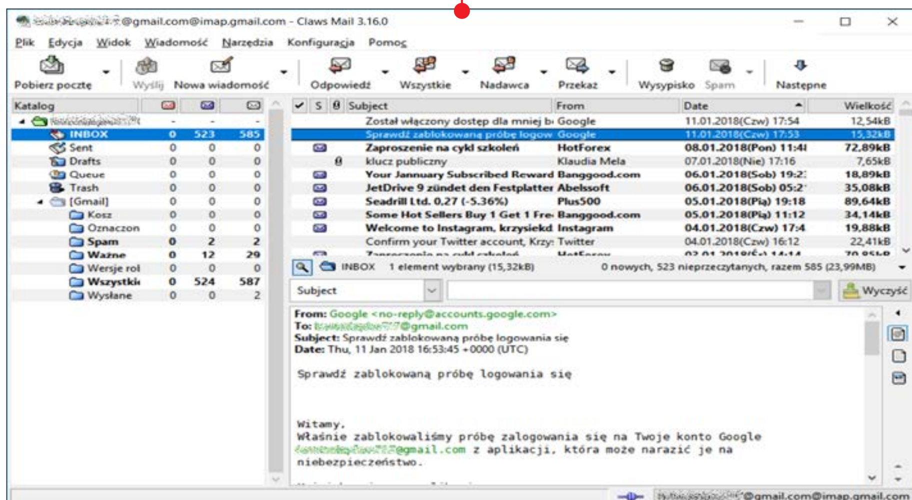


Mozilla Thunderbird

Jest to jeden z najlepiej rozwiniętych klientów poczty e-mail dostępnych za darmo i opartych na licencji Open Source. Z Thunderbirda można korzystać na co dzień, a nie tylko wtedy, gdy zależy nam na prywatności – to uniwersalne rozwiązanie. Możemy w nim podłączyć do jednej skrzynki wiele kont pocztowych i synchronizować wszystkie nasze wiadomości. E-maile można sortować i nadawać im priorytety. Dużym plusem jest możliwość instalowania dodatków, które rozszerzają możliwości tego klienta poczty. Dodają nowe funkcje lub zwiększają komfort korzystania z Thunderbirda. Całkowitą konfigurację tego klienta i sposób szyfrowania wiadomości poznamy w rozdziale szóstym.

Claws Mail

Jest to minimalistyczny klient poczty e-mail. Jego największą zaletą jest szybka praca nawet na starszych maszynach. Nie wykorzystuje zbyt dużo zasobów komputera. Zapewnia znacznie mniej funkcji niż Thunderbird, jednak znacznie szybciej wczytuje wiadomości i jest bardziej intuicyjny w obsłudze. Zobaczmy, jak skonfigurować tego klienta do pracy.

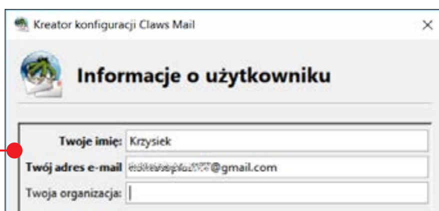




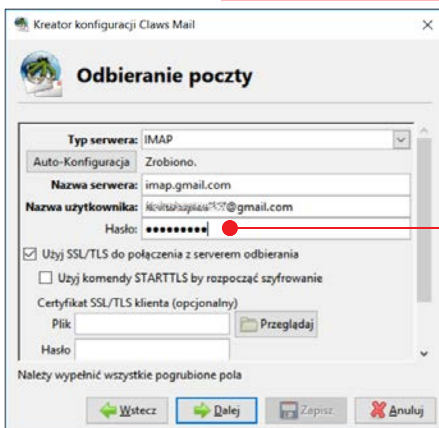
1 Po zainstalowaniu uruchamiamy program Claws Mail. Od razu pojawi się kreator konfiguracji. W jego oknie klikamy na **Dalej** ●.

2 Następnie podajemy nasze imię oraz adres e-mail ●, który chcemy dodać do klienta Claws Mail, i klikamy na **Dalej**.

3 Teraz wybieramy typ serwera **IMAP** i klikamy na **Auto-Konfiguracja**. Jeśli chcemy



automatycznie logować się do tej skrzynki, możemy od razu podać hasło dostępu do konta w polu **Hasło** ●. Resztę ustawień po-



POP3 A IMAP

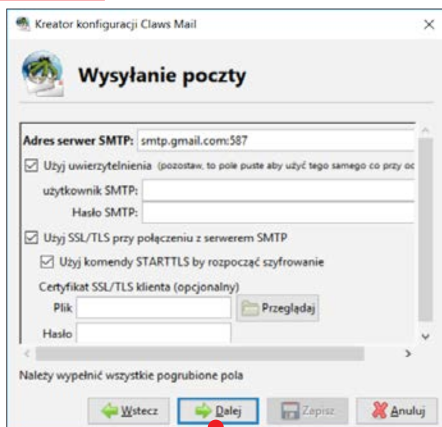
Są to protokoły służące do odczytu poczty z serwera. W większości przypadków każdy może korzystać z jednego lub drugiego protokołu – wybór jest wolny. Warto jednak znać różnice pomiędzy tymi protokołami.

■ **POP3 – Post Office Protocol 3** – jest to protokół przeznaczony raczej do pracy offline. Po zestawieniu połączenia cała zawartość naszej skrzynki, wraz z załącznikami, jest pobierana na nasz komputer. W zależności od ustawień serwera wiadomości są wtedy z niego usuwane lub pozostawiane. Takie rozwiązanie miało sens kiedyś, gdy dostęp do internetu był bardziej utrudniony i praca była wykonywana z jednego komputera.

■ **IMAP – Internet Message Access Protocol** – ten protokół działa w zupełnie inny sposób. Cała poczta jest zawsze przechowywana na serwerze pocztowym. Po zestawieniu połączenia na nasz komputer kopiowana jest struktura skrzynki pocztowej i same nagłówki wiadomości. Przesłanie treści i załączników następuje dopiero po otworzeniu danej wiadomości. Po wybraniu tego protokołu można pracować na wielu komputerach i różnych urządzeniach, gdyż na każdym będziemy widzieli odczyt z głównego serwera pocztowego. Oczywiście przy tym protokole wymagane jest ciągłe połączenie z internetem do przeglądania skrzynki pocztowej.

zostawiamy bez zmian i klikamy na przycisk **Dalej**.

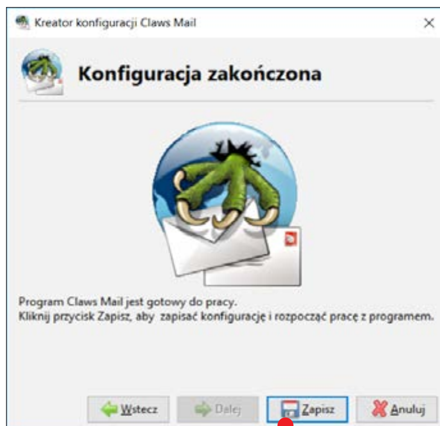
4 Następne okno zawiera opcje konfiguracyjne poczty wychodzącej. W naszym przykładzie zostawiamy domyślne ustawienia – powinny być odpowiednie dla większości użytkowników, wystarczy więc kliknąć na **Dalej**.



5 W ostatnim oknie kreatora klikamy na polecenie **Zapisz**.

Szyfrowanie poczty

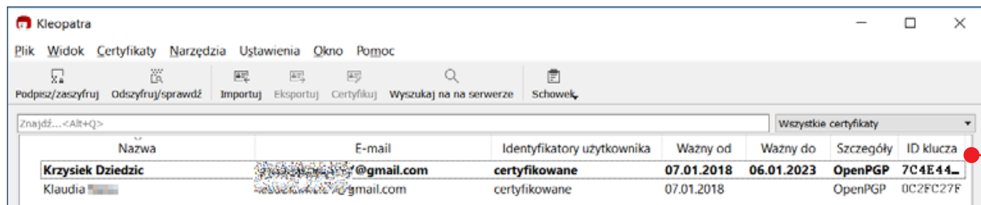
Oprócz samego klienta poczty i skrzynki pocztowej potrzebny nam będzie jeszcze program do szyfrowania wiadomości. Potrzebujemy aplikacji do zarządzania kluczami, które są niezbędne przy protokołach szyfrujących typu OpenPGP. Do rozpoczęcia wymiany zaszyfrowanych wiadomości niezbędne jest wygenerowanie specjalnego klucza prywatnego i publicznego, następnie musimy wymienić się z naszymi rozmówcami kluczami publicz-



nymi i dodać ich do zaufanych odbiorców. Wtedy, po skonfigurowaniu klienta pocztowego, będziemy mogli wysyłać wiadomości tak jak do tej pory, ale będą one automatycznie szyfrowane przy wysyłaniu i rozszyfrowywane przy odbieraniu. Użytkownikom nie przysparza to żadnych dodatkowych trudności, więc warto z tego korzystać. Konfigurację programów **Thunderbird** i **Enigmail** znajdziemy w rozdziale szóstym, a poniżej – opis **Gpg4win** niezbędnego do działania Enigmail i innych aplikacji szyfrujących wymagających kluczy prywatnych i publicznych.

Gpg4win

Jest to unikatowy program, który sprawdza się doskonale w Windows. Większość tego typu aplikacji jest tworzona pod systemy Linux, ten jako jeden z nielicznych jest najczęstszym wyborem osób korzystających z systemu Microsoftu. Składa się z kilku modułów, o których instalacji możemy sami zdecydować. Samo generowanie kluczy, ich eksport i import są proste. Wszystkie operacje można wykonać

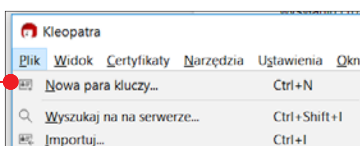


bardzo szybko i w kilka kliknięć. Domyślnie tworzone certyfikaty z wykorzystaniem kluczy mają 2048 bitów długości, a standardowy algorytm szyfrowania i podpisywania to RSA.

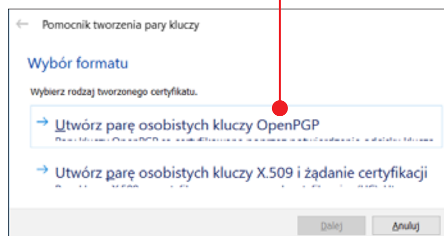
Generujemy klucze

1 Po zainstalowaniu programu Gpg4win z wszystkimi modułami otwieramy moduł **Kleopatra**.

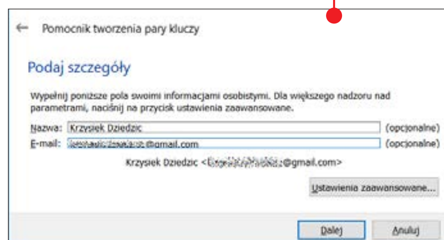
2 Następnie klikamy na **Plik**, **Nowa para kluczy**.



3 Wybieramy opcję **Utwórz parę osobistych kluczy OpenPGP**.

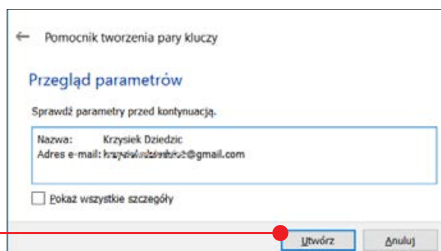


4 Następnie podajemy dane i klikamy na **Dalej**.

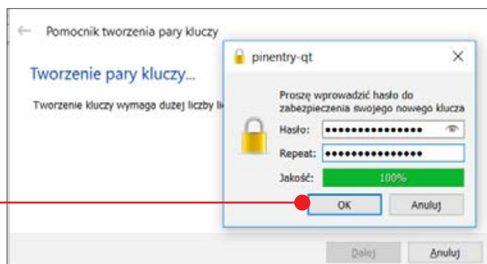


5 W następnym oknie klikamy na polecenie **Utwórz**.

6 Rozpocznie się tworzenie kluczy. Musimy jeszcze podać hasło, które będzie służyło



do zabezpieczenia klucza prywatnego, i kliknąć na **OK**. Na ostatnim ekranie klikamy na **Zakończ**.

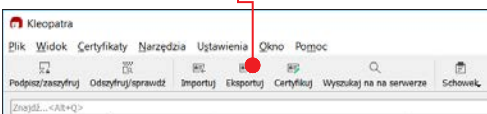


Eksport/Import kluczy

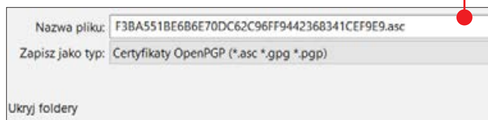
Jeśli zmieniamy komputer lub korzystamy z kilku, bardzo ważne jest, aby na każdym z urządzeń, z których będziemy wysyłać wiadomości, mieć zainstalowany program do obsługi kluczy, na przykład Gpg4win. Niezbędne będą nam również klucze wygenerowane na pierwszym urządzeniu. Możemy je swobodnie wyeksportować, a później na innym komputerze zaimportować. Dzięki temu będziemy mogli korzystać z zaszyfrowanych wiadomości na każdym naszym urządzeniu. Trzeba pamiętać, że musimy również wyeksportować klucze publiczne naszych odbiorców – inaczej nie będziemy w stanie prowadzić zaszyfrowanej korespondencji.

Eksport kluczy

1 W głównym oknie interfejsu programu Kleopatra wybieramy klucz, a następnie klikamy na **Eksportuj** na górnym pasku.

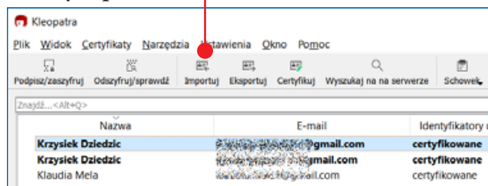


2 Zapisujemy certyfikat w wybranej lokalizacji na dysku, klikając na **Zapisz**.

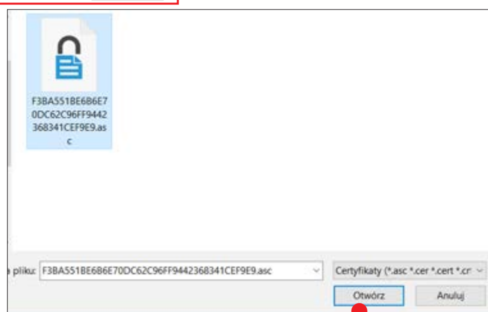


Import kluczy

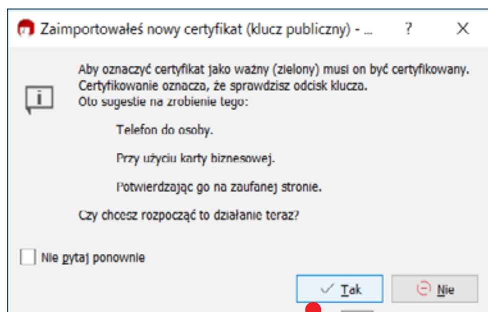
1 W głównym oknie interfejsu programu Kleopatra klikamy na **Importuj** na górnym pasku.



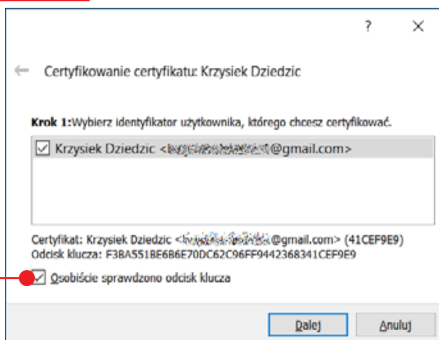
2 Wskazujemy certyfikat i klikamy na **Otwórz**.



3 W następnym oknie klikamy na przycisk **Tak**.



4 Teraz zaznaczamy pole przy identyfikatorze, który chcemy potwierdzić, i pole przy opcji **Osobiście sprawdzono odcisk klucza**, po czym klikamy na **Dalej**.



5 Następnie wystarczy kliknąć na **Certyfikuj**, podać hasło, zatwierdzić – i to koniec całego procesu.

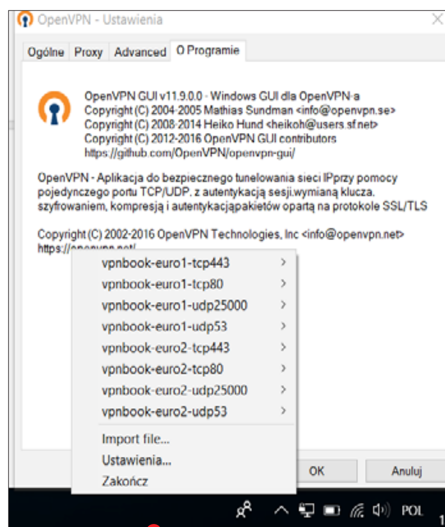
Klient VPN

Służy on do nawiązywania bezpiecznego szyfrowanego połączenia pomiędzy dwoma punktami – naszym komputerem i wybranym serwerem. Dzięki wykorzystaniu odpowiednich protokołów takie połączenie jest

ENIGMAIL

Jest to specjalny dodatek do klienta pocztowego Mozilla Thunderbird, który pozwala na implementację szyfrowania. Do pracy niezbędny jest również program zarządzający certyfikatami, jak Gpg4win. Zaletą Enigmail jest znacznie uproszczona konfiguracja i lepsze domyślne ustawienia generatora kluczy. Zamiast standardowego klucza o długości 2048 zostaje utworzony klucz o długości 4096, który jest praktycznie nie do złamania. Dodatkowo wymagania dotyczące tworzonego hasła zabezpieczającego klucz prywatny są znacznie wyższe, co wpływa na poprawę naszego bezpieczeństwa. Pełna konfiguracja tego dodatku jest opisana w dalszej części książki.

całkowicie bezpieczne i nie ma możliwości, aby osoby trzecie szpiegowały ruch naszych pakietów danych, dlatego też tego typu połączenia nazywa się popularnie **tunelowe**. Najpopularniejszym bezpiecznym programem, który zapewnia tego typu możliwości, jest OpenVPN.



■ **OpenVPN**
Ten program konfiguruje połączenie tunelowe z wykorzystaniem biblioteki **OpenSSL**. Obsługuje połączenia z uwierzytelnieniem kluczem, certyfikatem oraz loginem i hasłem. Jego konfiguracja nie należy do najprostszych, jednak możliwości ma znacznie większe niż konkurencyjne rozwiązania. Dodatkowo, większość tego typu aplikacji, w przeciwieństwie do OpenVPN, nie zapewnia nam anonimowości ani bezpieczeństwa, gdyż serwery i aplikacje są własnością firm i nie mamy pewności, czy nasz ruch danych nie jest analizowany. OpenVPN pozwala na skonfigurowanie pracy z wybranymi serwerami za darmo. Nie będziemy mogli wtedy korzystać z internetu z najwyższą przepustowością, jednak będziemy chronieni, nasz adres IP będzie ukryty i nie będziemy musieli płacić żadnych abonamentów. Pełny opis konfiguracji klienta OpenVPN znajdziemy w rozdziale szóstym.

Wyszukiwarki

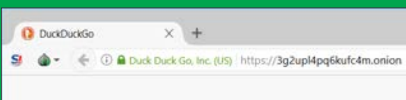
Zdecydowana większość użytkowników korzysta z dwóch wyszukiwarek – Google i Bing. Oferują one bardzo dużo, jednak odbywa się to pewnym kosztem. Po pierwsze wyświetlane są reklamy, a po drugie wyniki naszych wyszukiwań zapisywane są na serwerze i mogą być kolekcjonowane w celu utworzenia profilu reklamowego.

■ **DuckDuckGo**
Jest to jedna z nielicznych wyszukiwarek, która działa jako usługa dzięki wykorzystaniu modelu **SaaS** (Software as a Service). Dostępna jest pod adresem **https://duckduckgo.com**. Zasada takiej usługi opiera się na chmurze obliczeniowej. Wszystkie obliczenia, aktualizacje, zabezpieczenia są po stronie usłu-

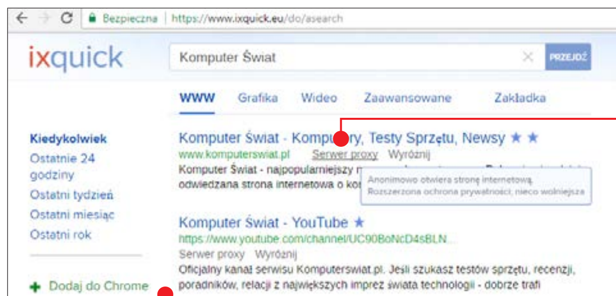


UKRYTA WYSZUKIWARKA

Jeśli korzystamy z przeglądarki Tor Browser, możemy skorzystać ze specjalnej „ukrytej" wersji tej wyszukiwarki dostępnej pod adresem **3g2upl4pq6kufc4m.onion** – adresy składające się z dziwnych ciągów zakończone rozszerzeniem **onion** należą do tak zwanych pseudodomen najwyższego poziomu. Dostęp do nich z poziomu zwykłej przeglądarki jest niemożliwy, gdyż nie są nazwami rozpoznawalnymi przez DNS i nie figurują w rejestrze TLD.

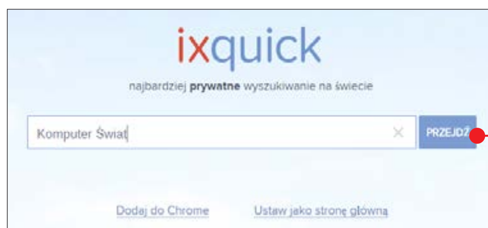


godawcy, klient tylko z nich korzysta. Anonimowość zapewnia rozproszenie po całym świecie wielu serwerów działających w tej usłudze, a wysłane przez nas zapytanie jest realizowane przez losowo wybrany serwer. Możemy również zainstalować specjalny dodatek do popularnych przeglądarek, który pozwoli nam na bardzo szybki dostęp do tej wyszukiwarki i jej integrację z wybraną przez nas przeglądarką.



Ixquick

Jest to wyjątkowa wyszukiwarka, oparta na meta silniku, który dostarcza wyniki z ponad 100 różnych źródeł z wyłączeniem Google. Dostępna jest pod adresem **https://www.ixquick.eu/**, a serwery znajdują się w Holandii. Oprócz szybkiego i bezpiecznego wyszukiwania bez przechowywania żadnych informacji na nasz temat udostępnia również możliwość łączenia się z wybranymi stronami poprzez specjalne serwery proxy, które zapewniają anonimowość dzięki zmianie adresu IP.



1 Wchodzimy na stronę **https://www.ixquick.eu**, wpisujemy szukaną frazę i klikamy na **Przejdź**.

2 Następnie możemy po prostu kliknąć na wybrany wyszukany wynik i przenieśmy się do wybranej strony. Alternatywnie możemy kliknąć na **Serwer proxy** pod znalezionym wynikiem. Wtedy wybrana strona zostanie otworzona z przekierowaniem przez serwer proxy. Oznacza to, że na stronie nie zostanie zapisany nasz adres IP, a jedynie adres przyznany przez proxy, co pozwala na zachowanie anonimowości podczas przeglądania.

3 Strony otwarte w trybie proxy będą ładować się znacznie dłużej i nie wszystkie elementy mogą działać poprawnie.

Komunikatory

Popularne komunikatory, jak Hangouts, Messenger czy też Skype, może i są wygodne, jednak nie oferują żadnej anonimowości i przechowują wszystkie informacje na swoich serwerach. Wiadomości są przesyłane zabezpieczonym kanałem, jednak osoby trzecie mogą złamać taki protokół, jeśli mają dostęp do naszej sieci. Dlatego jeżeli zależy nam na prywatności i bezpieczeństwie przy wymianie wiadomości, lepiej wybrać jeden z bezpiecznych komunikatorów. W ich wypadku każda wiadomość jest szyfrowana i zabezpieczana, a odszyfrowanie może nastąpić tylko



u adresata naszej wiadomości. W rozdziale szóstym omówiony zostanie zamiennik programu Skype – **Jitsi**.

Cryptocat

Ten komunikator zapewnia całkowite szyfrowanie każdej wiadomości dzięki **end-to-end encryption**. Pozwala na wysyłanie wiadomości, nawet gdy ich odbiorcy są niedostępni. Możemy instalować aplikację Cryptocat na wielu urządzeniach. Jest to dość prosty program, jednak umożliwia oprócz czatowania wysyłanie plików, które również są zaszyfrowane tak, że nikt nie podejrzy ich zawartości. Obsługa jest prosta, jednak by się komunikować, każdy użytkownik musi założyć konto i korzystać z aplikacji Cryptocat.

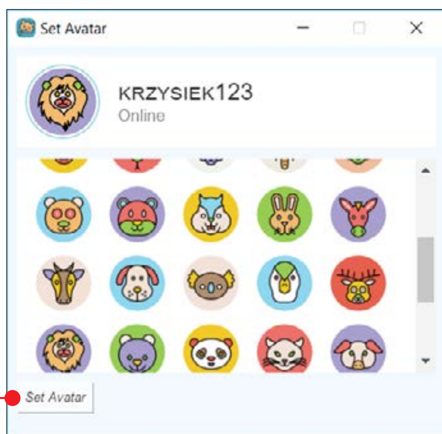
1 Po zainstalowaniu programu Cryptocat uruchamiamy go i klikamy na **Create Account**.

2 Otworzy się strona w przeglądarce, na której musimy podać dane potrzebne do utworzenia konta. Wymagane jest silne hasło, przynajmniej 12-znakowe. Po podaniu danych klikamy na **Create User**.

3 Jeśli login nie jest zajęty, konto zostanie utworzone. Wracamy do aplikacji i podajemy dane naszego konta. Klikamy na **Login**.

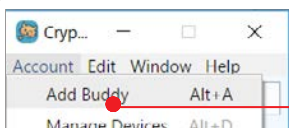
4 Następnie musimy potwierdzić, że urządzenie, z którego się logujemy, jest zaufane, klikając na **Continue**.

5 Następnie wybieramy ikonę urządzenia, z jakiego korzystamy, podajemy nazwę, jaką chcemy do niego przypisać, i klikamy na **Add Device**.



6 Pozostaje nam jeszcze wybranie awatara i kliknięcie na **Set Avatar**.

7 Dodajemy znajomych poprzez kliknięcie na **Account**, **Add Buddy**, następnie wpisujemy nazwę konta znajomego i wysyłamy zaproszenie.



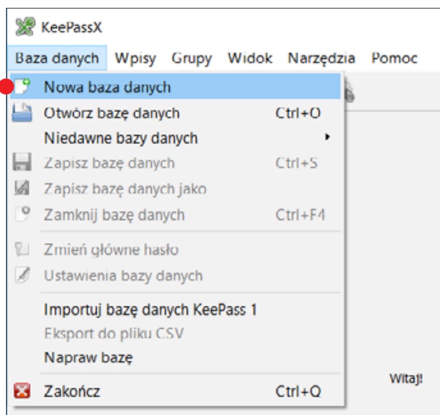
Menedżery haseł

Im więcej mamy różnych kont, tym trudniej zapanować nad wszystkimi hasłami. Dodatkowo, żeby być bezpiecznym, powinniśmy korzystać z rozbudowanych i skomplikowanych haseł, których zapamiętanie może sprawiać problem. Dlatego warto korzystać z bezpiecznego menedżera haseł, który pozwoli na dodawanie haseł do listy wraz z ich opisem. Możemy traktować takie rozwiązanie jak sejf, w którym znajdują się nasze dane dostępowe. Dzięki niemu zamiast kilkunastu haseł musimy pamiętać tylko jedno, skomplikowane i złożone, które potrzebne jest do otworzenia sejfu.

■ KeePassX

To najbardziej wiarygodny menedżer haseł, który działa bez problemów w systemie Windows. Pozwala nie tylko na zapisywanie haseł, ale też na przechowywanie różnego typu załączników, stron internetowych, loginów i komentarzy. Jego obsługa jest bardzo prosta, a konfiguracja i użytkowanie nie powinno sprawić problemu.

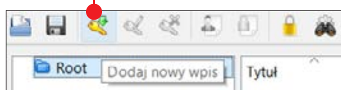
1 Po uruchomieniu programu KeePassX klikamy na **Baza danych**, **Nowa baza danych**.



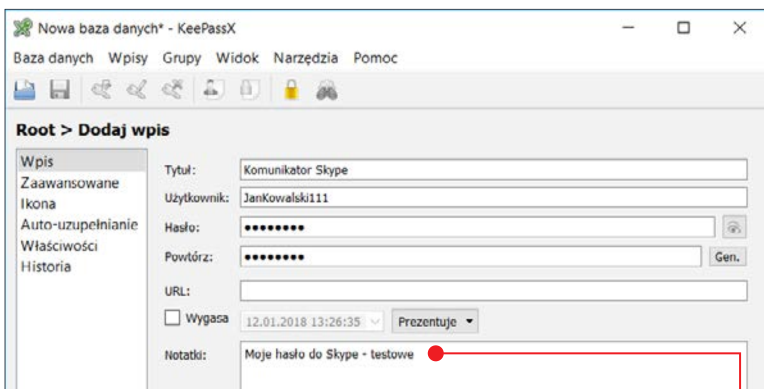
2 Podajemy hasło główne i klikamy na **OK**. Opcjonalnie możemy dodatkowo stworzyć klucz.



3 Następnie dodajemy nowe hasła i informacje, klikając na **Nowy wpis** i podając odpowiednie dane.

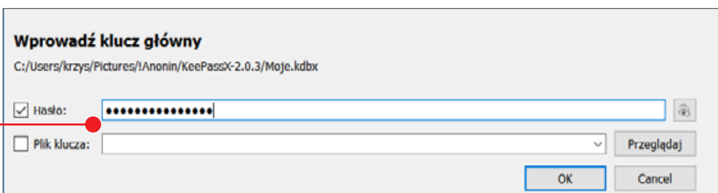


4 Możemy wpisać wszystkie dane wraz z notatką, a nawet wybrać ikonę dla naszego wpisu. Zatwierdzamy wszystko, klikając na **OK**.



5 Przy zamykaniu programu będziemy musieli zapisać naszą bazę danych i nadać jej nazwę.

6 Przy kolejnym uruchomieniu zawsze będzie wybierana ostatnio używana baza. Do jej otworzenia będziemy potrzebowali utworzonego wcześniej hasła i ewentualnie pliku klucza.

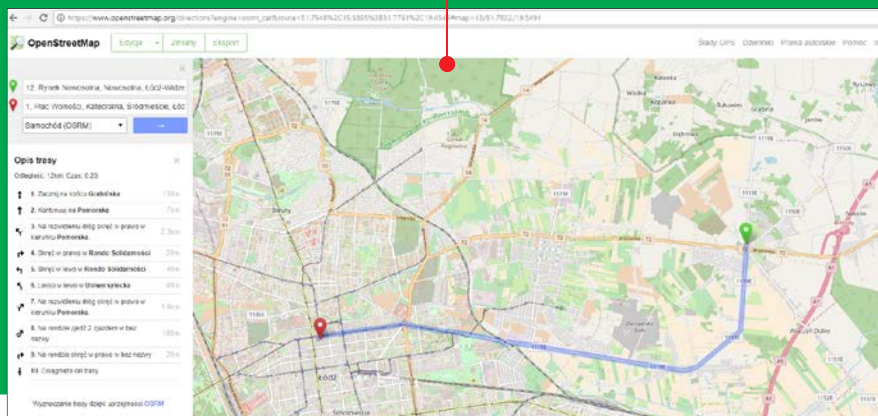


OTWARTE MAPY

Warto skorzystać z alternatywy do Google Maps, Apple Maps czy też Bing Maps – czyli z **OpenStreetMap**. Będziemy mogli dokładnie sprawdzić wybraną lokalizację oraz wyznaczyć trasę dojazdu. Możemy też wybierać różnego rodzaju warstwy, na przykład transport publiczny czy ścieżki rowerowe. Co najciekawsze, możemy aktywnie przyczynić się do tworzenia mapy i samemu dodawać wpisy. Największą zaletą otwartych map jest brak śledzenia użytkownika, zbierania informacji na jego temat i wykorzystywania historii podróży do rekomendowania reklam itp.



Warto również przetestować aplikację **OsmAnd** dostępną na smartfony, która korzysta właśnie z otwartych map. Mamy możliwość pobrania wybranego obszaru i korzystania z nawigacji offline.



3 Zacieramy ślady w komputerze

PROGRAMY OPISANE W TYM ROZDZIALE ZNAJDZIESZ NA DVD

Nasz komputer to kopalnia informacji o nas. Jeśli ktoś uzyska do niego dostęp, może bardzo szybko zdobyć hasła i prywatne pliki oraz wiele się o nas dowiedzieć. W tym rozdziale przeczytamy, jak zadbać o wrażliwe dane i usunąć ślady, które zostawiamy, korzystając z komputera

Usuwamy historię przeglądania i inne ślady oraz pliki cookie

Większość użytkowników przeglądarek internetowych nawet nie zdaje sobie sprawy, jak wiele informacji na ich temat jest gromadzonych zarówno na samym komputerze, jak i w serwisach, do których się logują. Jest to z pewnością bardzo wygodne, gdy możemy uzyskać dostęp do odwiedzonych wcześniej witryn na smartfonie czy też automatycznie logować się do wielu stron. Jednak zwiększa to również ryzyko uzyskania przez osoby trzecie dostępu do naszych kont i profili.
Wystarczy, że ktoś usiądzie przy naszym laptopie lub pececie na kilka chwil i już może poznać nasze hasła do wielu usług.
Dlatego, jeśli z naszego komputera może skorzystać ktoś poza nami, bardzo istotne jest dbanie o to, żeby nasze hasła nie były zapisywane przez przeglądarkę i by wyniki naszych wyszukiwań były usuwane.
Zobaczmy na przykładzie kilku popularnych przeglądarek, jak pozbyć się historii i innych śladów, jakie zostawiamy, oraz plików cookie.



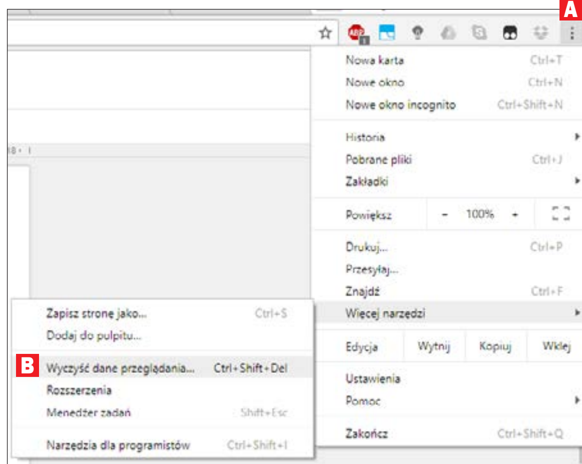
Google Chrome

W Chrome możemy skasować wszystkie wspomniane informacje w jednym menu, co jest bardzo wygodne. Dodatkowo warto pamiętać, że jeśli nie chcemy, żeby przeglądarka zapisywała dane z jakiejś sesji, powinniśmy uruchomić tryb incognito.

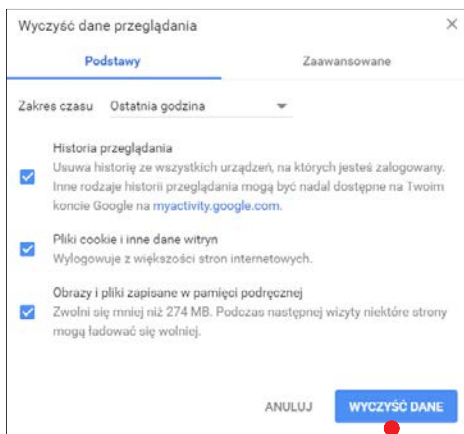
1 Usuwanie historii przeglądania jest bardzo proste. Po uruchomieniu Chrome klikamy na trzy kropki w górnym prawym rogu **A**.

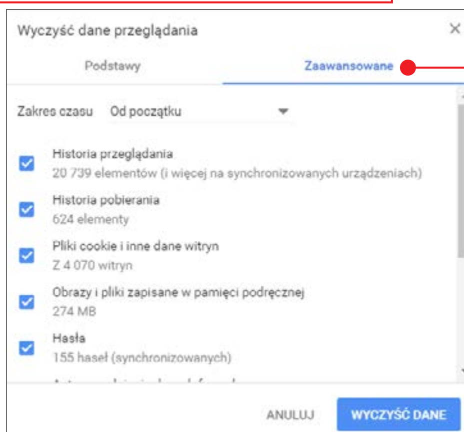
2 Następnie najeżdżamy kursorem na **Więcej narzędzi** i klikamy na **Wyczyść dane przeglądania** **B**.

3 Teraz możemy wybrać zakres czasu, z jakiego chcemy wymazać dane, i kliknąć



na **WYCZYŚĆ DANE**. Nie skasujemy jednak w ten sposób wszystkich informacji. Musimy jeszcze kliknąć na **Zaawansowane**.





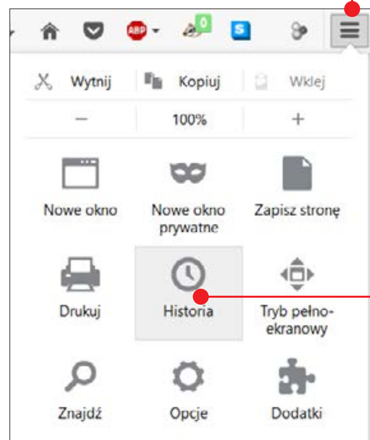
4 W oknie **Zaawansowane** wybieramy zakres czasu – **Od początku**, a następnie zaznaczamy wybrane opcje i klikamy na **WYCZYŚĆ DANE**.
W naszym przykładzie po kilku miesiącach użytkowania przeglądarki Chrome na kilku urządzeniach było w niej zapisanych aż 155 haseł.



Mozilla Firefox

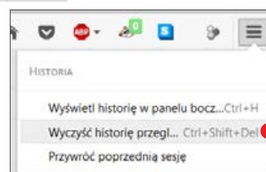
W przeglądarce Firefox również możemy wyczyścić wszystkie dane, korzystając z jednego menu.

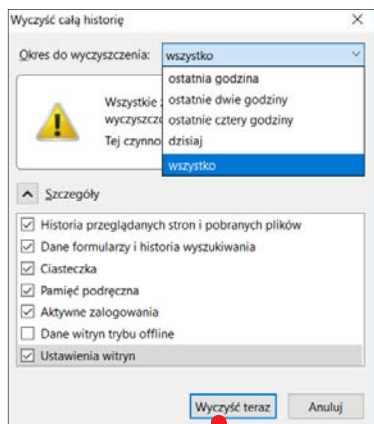
1 Po uruchomieniu przeglądarki klikamy w górnym prawym rogu okna na ikonę menu – trzy kreski.



2 Następnie z rozwiniętej listy opcji wybieramy pozycję **Historia**.

3 Teraz klikamy na **Wyczyść historię przeglądania**.





4 Następnie wybieramy z listy **Okres do wyczyszczenia** odpowiedni czas i klikamy na **Szczegóły**. Zaznaczamy, jakie dane mają zostać usunięte. Na koniec klikamy na **Wyczyść teraz**.



Edge

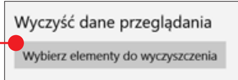
W najnowszej przeglądarce Microsoftu domyślnie dostępnej w systemie Windows 10 również możemy skasować wszystkie dane, korzystając z jednego menu. Dodatkowo możemy też zaznaczyć opcję, która pozwoli na automatyczne kasowanie wszystkich danych przy zamykaniu przeglądarki, co może okazać się bardzo przydatne. Niestety, nie można za to wybierać czasu, z jakiego dane mają zostać wyczyszczone.

1 Po uruchomieniu przeglądarki klikamy na trzy kropki w prawym górnym rogu.

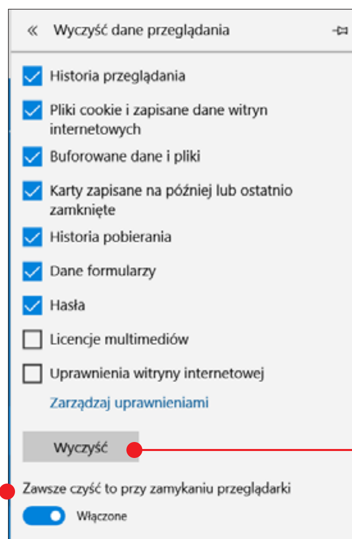
2 Następnie klikamy na **Ustawienia** na dole listy.



3 Teraz przewijamy menu aż do pozycji **Wyczyść dane przeglądania** i klikamy na **Wybierz elementy do wyczyszczenia**.



4 Możemy zaznaczyć wybrane elementy do wyczyszczenia, a także opcję automatycznego czyszczenia przy zamykaniu przeglądarki. Na koniec klikamy na polecenie **Wyczyść**.



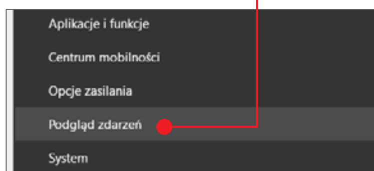
Dziennik systemowy – jakie dane w nim się znajdują i jak go wyczyścić

Zacznijmy od tego, czym jest dziennik zdarzeń w systemie Windows, czyli funkcja o nazwie **Podgląd zdarzeń**. Otóż jest to składnik systemu, który odpowiada za przechowywanie wszelkiego typu informacji dotyczących aktywności komputera.

Wpisy, które są w nim tworzone, odnoszą się do uruchamianych usług, włączania ważnych aplikacji, a nawet wciskania fizycznego przycisku zasilania. Jest to bardzo przydatne narzędzie, które może pomóc nam zdiagnozować problemy występujące w naszym systemie czy w komputerze. Może jednak także stać się źródłem wiedzy na nasz temat – w dzienniku zapisywane są dokładne czasy wszystkich ważnych akcji. Dzięki temu ktoś, kto uzyska dostęp do podglądu zdarzeń, będzie w stanie określić dokładnie, w jakich godzinach korzystaliśmy z komputera, kiedy go uruchomiliśmy i wyłączyliśmy. Z punktu widzenia zachowania prywatności warto co jakiś czas czyścić wpisy dziennika systemowego, zwłaszcza jeśli nie występują żadne problemy techniczne w naszym urządzeniu.

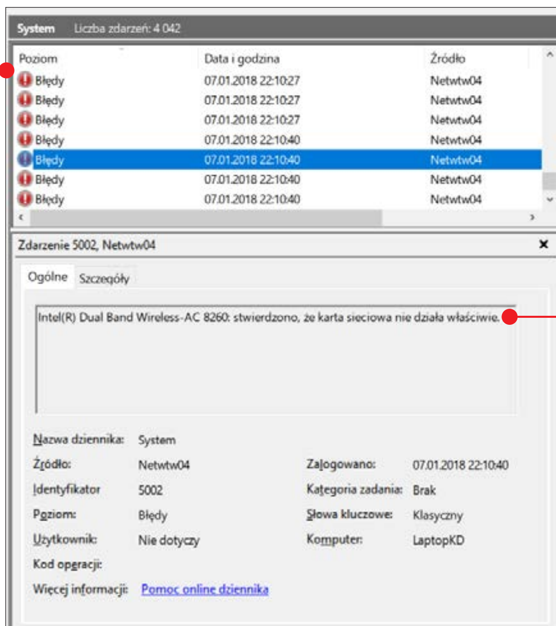
Uruchamiamy podgląd zdarzeń

1 Klikamy prawym przyciskiem myszy na menu **Start**, a następnie z listy wybieramy opcję **Podgląd zdarzeń**.



2 Teraz po lewej stronie zauważymy drzewo katalogów. Wszystkie zapisywane zdarzenia są umieszczane w odpowiednich katalogach, dzięki czemu łatwiej dotrzeć do tego, czego szukamy. **Uwaga!** Nie należy się przejmować nawet większą ilością powtarzających się błędów

i ostrzeżeń – zdecydowana większość takich błędów jest nieszkodliwa. Jeśli nasz komputer działał do tej pory bez żadnych problemów, nie powinniśmy się nimi przejmować. Możemy się nimi bardziej zainteresować dopiero w sytuacji, gdy komputer na przykład sam się wyłącza lub zaczną przeszkadzać nam inne problemy.

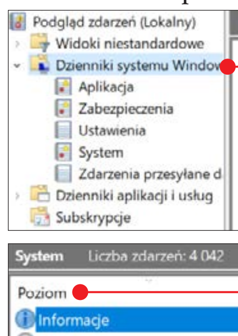


Korzystamy z podglądu zdarzeń i dzienników

Ta funkcja systemu Windows przydaje się głównie do diagnostyki, ponieważ odnotowuje błędy występujące w systemie oraz, jak już wiemy, pozwala sprawdzić, kto, w jakich godzinach i w jaki sposób korzystał z komputera.

Analizujemy błędy

1 Po uruchomieniu Podglądu zdarzeń po lewej stronie klikamy na strzałkę przy kategorii **Dzienniki systemu Windows**, w celu jej rozwinięcia.

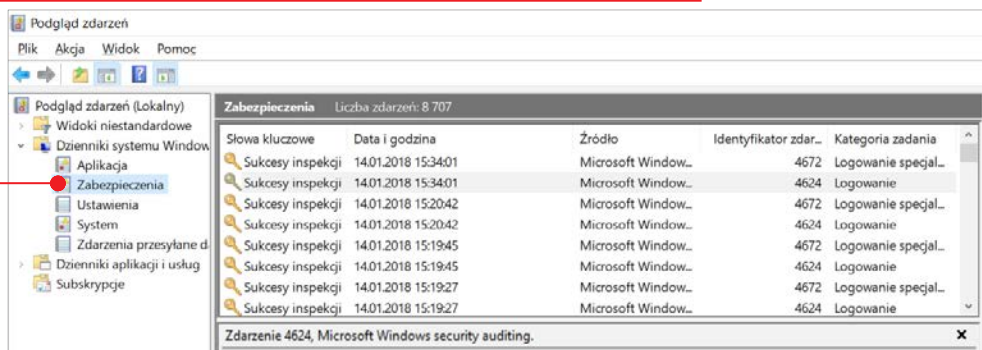


2 Teraz przechodzimy do wybranej zakładki, na przykład **System**, i klikamy na **Poziom** w celu posortowania informacji i łatwiejszego odnalezienia błędów.

3 Po znalezieniu błędu i kliknięciu na niego na dole ekranu pojawią się szczegółowe informacje modułu lub aplikacji, która sprawia problem. Dzięki temu możemy szukać dalszej pomocy w sieci, podając również identyfikator błędu i jego źródło.

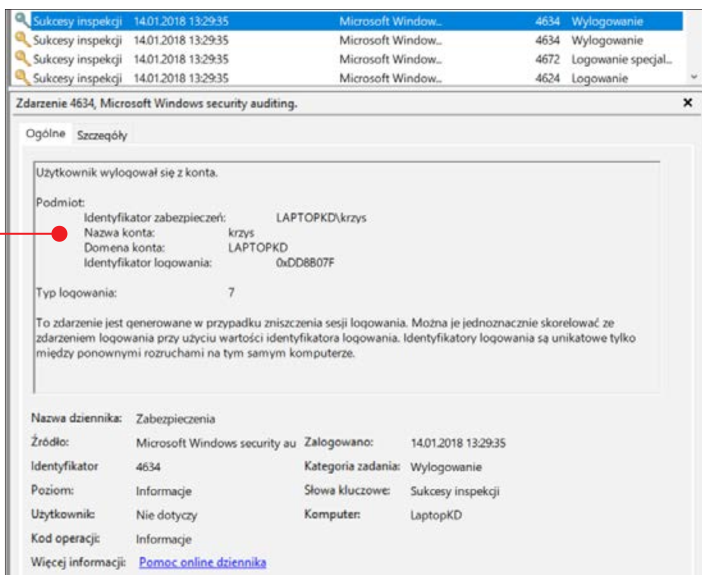
Sprawdzamy czas aktywności komputera

1 Najprościej sprawdzić tego typu informacje, rozwijając w dzienniku pozycję **Zabezpieczenia**.



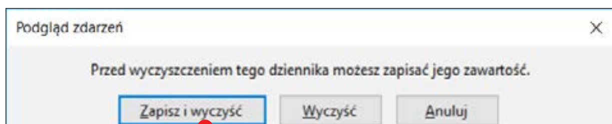
2 Interesują nas wpisy oznaczone jako kategoria zadania **Logowanie** lub **Wylogowanie**. Na tej podstawie jesteśmy w stanie bardzo precyzyjnie określić, kiedy, o jakiej godzinie i na jakie konto nastąpiło zalogowanie lub wylogowanie.

3 Po kliknięciu na dany wpis na dole okna będziemy mogli sprawdzić szczegóły wpisu do dziennika.

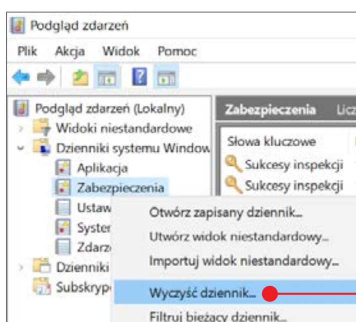


Usuwamy dane z dzienników systemowych

1 Klikamy prawym przyciskiem myszy w oknie po lewej stronie na wybrany dziennik, następnie z listy wybieramy opcję **Wyczyść dziennik**.

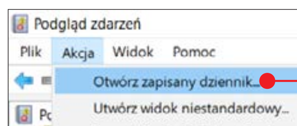


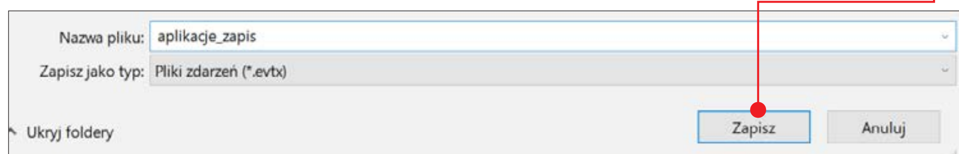
2 Jeśli chcemy zapisać dane do późniejszej diagnostyki w przypadku wystąpienia problemów, wybieramy opcję **Zapisz i wyczyść** (jeżeli wolimy niczego nie zachowywać, po prostu klikamy na **Wyczyść**).



3 Zapisujemy plik z dziennikiem na dysku, a w podglądzie zdarzeń dziennik zostanie wyczyszczony.

4 Zapisany dziennik możemy w każdej chwili otworzyć, klikając na **Akcja**, **Otwórz zapisany dziennik**.





Wykrywamy i usuwamy programy wykradające nasze dane

Bardzo dużym zagrożeniem dla naszej prywatności są złośliwe programy zainstalowane w komputerze oraz ukryte wirusy, które zbierają informacje na nasz temat i wysyłają je do internetu. Mogą to być keyloggery, które zapisują wciskane klawisze, aplikacje wyświetlające reklamy i oferujące instalowanie płatnych usług i wiele innych uciążliwych lub niebezpiecznych aplikacji. Zdarza się, że pomimo ochrony programu antywirusowego takie szkodniki przedostają się na dysk. Najlepiej zainstalować specjalny program do usuwania tego typu oprogramowania – na przykład **Malwarebytes**.

Walka ze szkodliwym oprogramowaniem

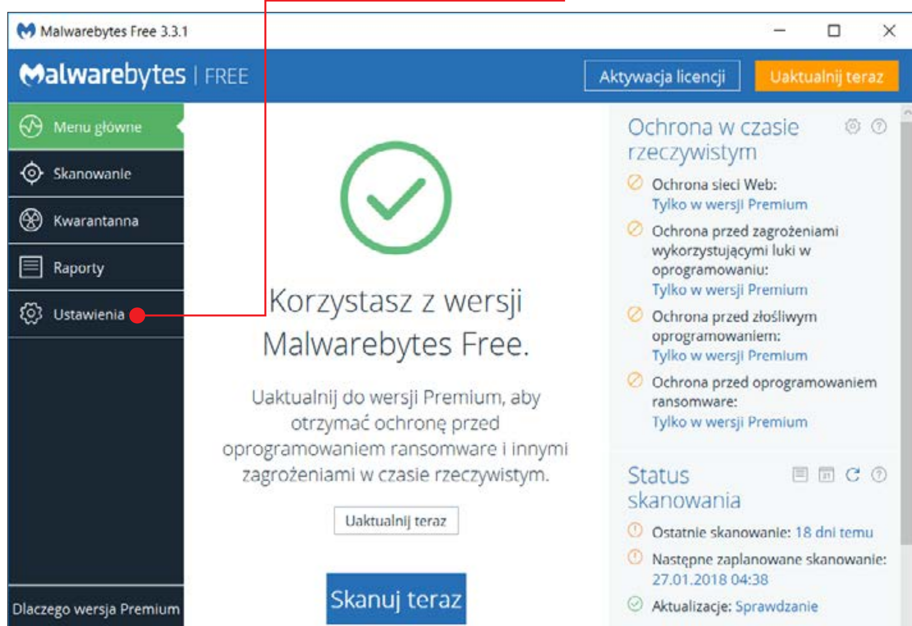
Malwarebytes to specjalny program, którego zadaniem jest wykrywanie niebezpiecznego, złośliwego oprogramowania. Dotyczy to rootkitów, trojanów i wielu innych zagrożeń. Ważną dodatkową opcją jest również wykrywanie aplikacji typu **PUP**, czyli potencjalnie niepożądanych programów – teoretycznie działają one normalnie, jednak mogą zagrażać wygodzie i bezpieczeństwu użytkownika przez oferowanie reklam i zbieranie informacji na jego temat.

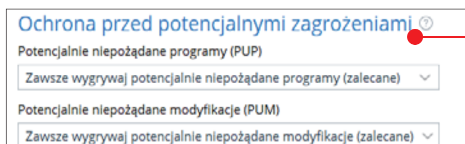
Obsługa Malwarebytes jest bardzo prosta. Wystarczy przeskanować komputer raz na tydzień, żeby zadbać o bezpieczeństwo.

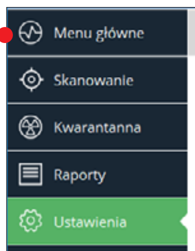
Ustawiamy skaner

1 Instalujemy i uruchamiamy program Malwarebytes.

2 W głównym oknie klikamy na **Ustawienia** po lewej stronie.







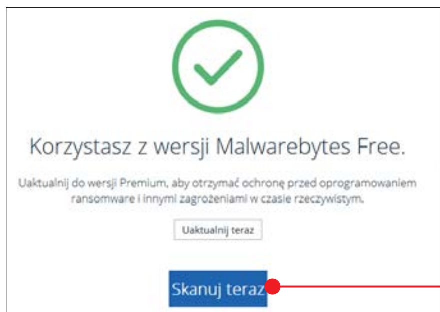
3 Przechodzimy do zakładki **Ochrona** i przewijamy widok okna aż do kategorii **Ochrona przed potencjalnymi zagrożeniami**.

4 Ustawiamy ochronę przed **PUP** i **PUM** jako aktywną, a potem wracamy do głównego okna, klikając na **Menu główne** po lewej stronie.

Korzystamy ze skanera

1 Uruchamiamy program Malwarebytes.

2 Upewniamy się, że mamy aktywne połączenie z internetem, które jest



niezbędne do pobrania najnowszych sygnatur zagrożeń.

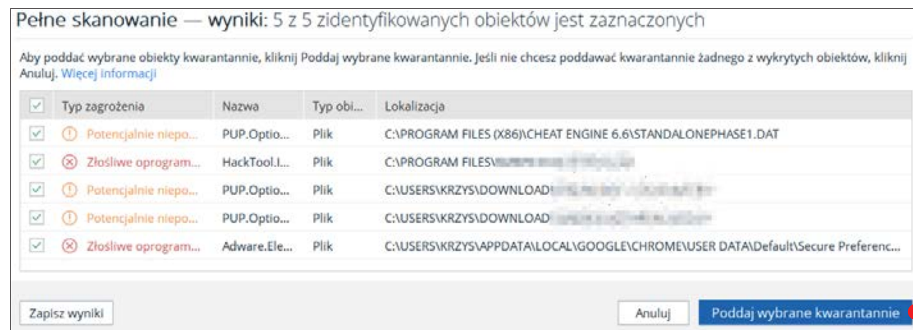
3 W głównym oknie programu klikamy na **Skanuj teraz**.

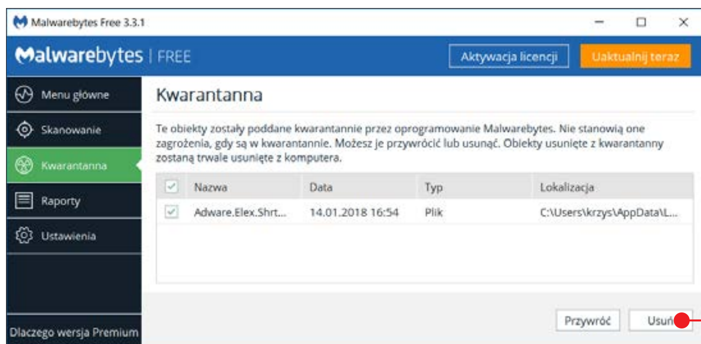
4 Rozpocznie się skanowanie, które może potrwać bardzo długo w zależności od rozmiaru naszych dysków.

5 Na koniec zostanie przedstawiony raport ze znalezionymi zagrożeniami. Możemy sami zweryfikować zidentyfikowane obiekty. Aby przejść dalej, klikamy na **Poddaj wybrane kwarantannie**. Dzięki temu nie będziemy dłużej zagrożeni.

6 Jeśli nie zaznaczyliśmy wybranych obiektów, zostaniemy

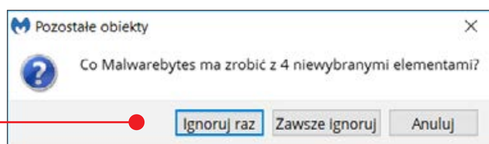


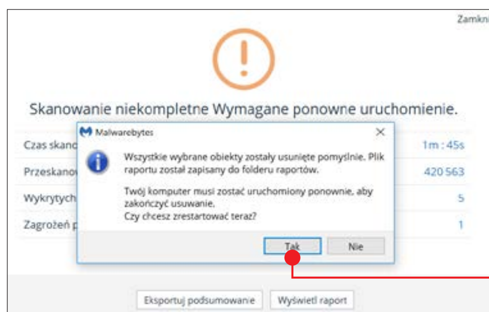




zapytani, czy chcemy zawsze je ignorować, czy tylko tym razem. Klikamy na opcję, która nam odpowiada.

7 W większości przypadków, aby przenieść zagrożenie do kwarantanny, wymagane będzie ponowne uruchomienie komputera. Klikamy na **Tak**.





8 Po restarcie komputera uruchamiamy program Malwarebytes i przechodzimy do zakładki **Kwarantanna**.

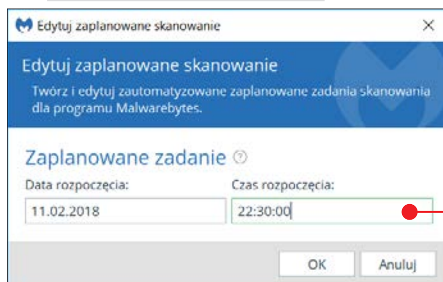
9 Po prawej stronie znajdziemy wszystkie zagrożenia, możemy teraz ostatecznie podjąć decyzję o neutralizacji zagrożenia poprzez wybranie go i kliknięcie na **Usuń** w prawym dolnym rogu.

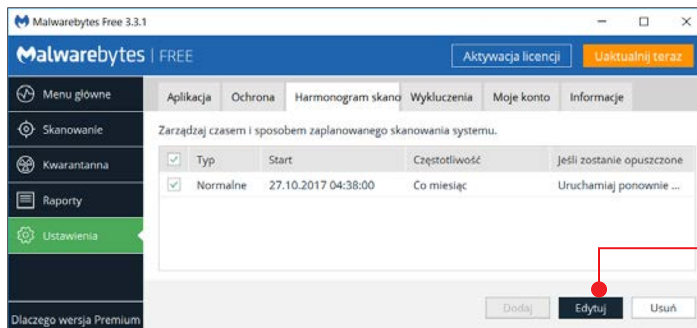
Harmonogram skanowania

W darmowej wersji programu mamy dostęp do jednego harmonogramu zdefiniowanego na comiesięczne skanowanie, możemy ustalić dzień i godzinę rozpoczęcia skanowania.

1 Klikamy na **Ustawienia** w głównym oknie programu.

2 Następnie przechodzimy do zakładki **Harmonogram skanowania**.





3 Zaznaczamy dostępne zadanie skanowania i klikamy na **Edytuj** u dołu okna.

4 Ustalamy datę, godzinę i na koniec klikamy na **OK**.

Czyścimy plik wymiany przy zamykaniu komputera

Plik wymiany przechowywać może bardzo wiele informacji dotyczących naszej ostatniej sesji. Można go odczytać i odkryć, nad czym ostatnio pracowaliśmy i jakie pliki były otwierane. Dla zwiększenia bezpieczeństwa i ochrony prywatności możemy skonfigurować system tak, aby czyścił zawartość tego pliku przy zamykaniu.

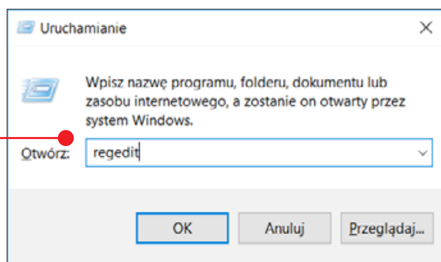
Plik wymiany, czy też stronicowania, służy w systemie Windows jako rozszerzenie pamięci RAM. Jeśli mamy jej zbyt mało, dane zapisywane są na naszym dysku właśnie w pliku wymiany, który jest traktowany jako wirtualny RAM. Dzięki temu komputer nadal pracuje w miarę stabilnie bez zawieszania się, możemy jednak odczuć spowolnioną pracę dysku, który będzie w ciągłym użyciu. Wszelkie dane zapisane w pamięci RAM są automatycznie usuwane przy wyłączaniu zasilania – gdy kości pamięci nie mają zasilania, przechowywane dane zostają zapomniane. W przypadku pliku stronicowania jest jednak inaczej. Dostęp do zapisanych danych jest bardzo prosty i nie są one domyślnie czyszczone.

Możemy sami skonfigurować system Windows do czyszczenia tego pliku przy każdym zamknięciu systemu, co zwiększy nasze bezpieczeństwo i uniemożliwi sprawdzenie naszej aktywności w ostatniej sesji. Wadą takiego rozwiązania jest możliwe spowolnienie czasu zamykania systemu. Z drugiej jednak strony będziemy mogli zaobserwować minimalne zredukowanie czasu potrzebnego na rozruch. A w większości przypadków istotny jest raczej czas startu komputera, a nie jego zamknięcia.

Wprowadzamy zmiany

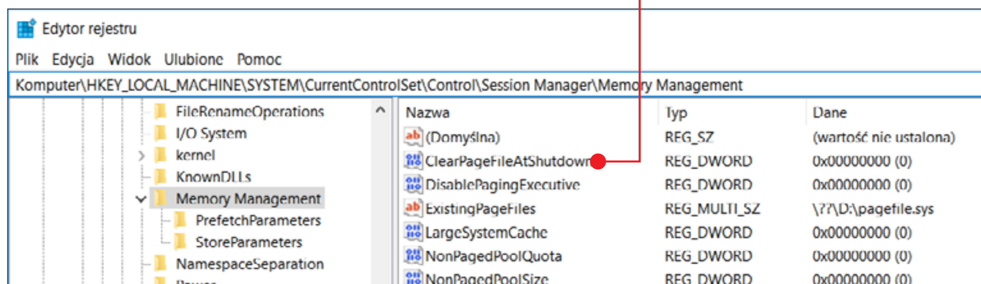
1 Wciskamy jednocześnie klawisze [Win]+[R].

2 Wpisujemy w pole okna **Uruchamianie** – **regedit** i klikamy na **OK**. Musimy również potwierdzić uprawnienia administratora.

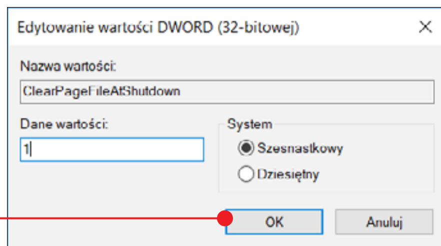


3 Następnie przechodzimy do klucza: **Komputer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management**

4 Teraz po prawej stronie klikamy dwukrotnie na wartość: **ClearPageFileAtShutdown**.



5 Zmieniamy domyślne dane wartości z 0 na **1** i klikamy na **OK**.



6 Od teraz przy zamykaniu systemu plik wymiany będzie czyszczony automatycznie.
W każdej chwili możemy cofnąć zmiany, powtarzając kroki tej porady – podając w danych wartości **0** zamiast 1.

Szyfrowanie systemu Windows

Najlepszą ochroną prywatności jest zabezpieczenie naszego dysku poprzez wprowadzenie szyfrowania. Wtedy jeśli na przykład nasz laptop zostanie skradziony i ktoś będzie chciał uzyskać dostęp do danych bez naszej wiedzy, będzie to praktycznie niemożliwe. Jedyna słabość takiego rozwiązania to błąd ludzki, czyli nasz. Jeśli przez przypadek powiemy komuś, jakie mamy hasło, lub zapiszemy je na kartce, żeby nie zapomnieć, a kartka trafi w niepowołane ręce – wtedy nasze dane będą zagrożone. W innym przypadku nie ma szans na złamanie odpowiednio długiego i mocnego hasła.

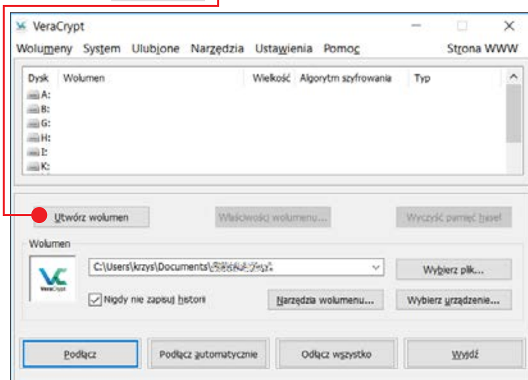
Wybrane foldery czy cały dysk?

Oczywiście z punktu widzenia bezpieczeństwa zalecane jest szyfrowanie całego dysku. Jednak wiąże się to ze spadkiem wydajności dysku w zależności od zastosowanego mechanizmu. Jeśli korzystamy z szybkiego nośnika SSD, zmiana nie powinna negatywnie wpłynąć na komfort korzystania z komputera, w przypadku mało wydajnych dysków twardych może to przeszkadzać. Jeśli zależy nam na wydajności i nie mamy potrzeby szyfrowania całego nośnika, możemy za pomocą programu VeraCrypt utworzyć specjalny magazyn, który będzie obejmować wybrany plik lub nawet partycję.

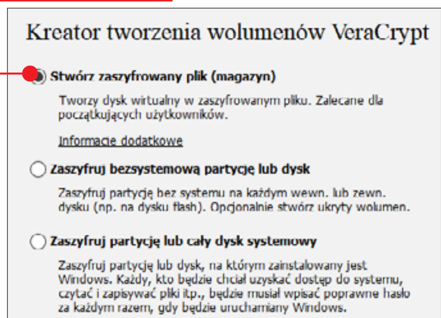
Tworzymy szyfrowany wolumen

1 Po zainstalowaniu uruchamiamy program **VeraCrypt**.

2 Najpierw klikamy na polecenie **Utwórz wolumen**.



3 W oknie kreatora pozostawiamy wybraną domyślnie opcję **Stwórz zaszyfrowany plik (magazyn)** i klikamy na **Dalej**.

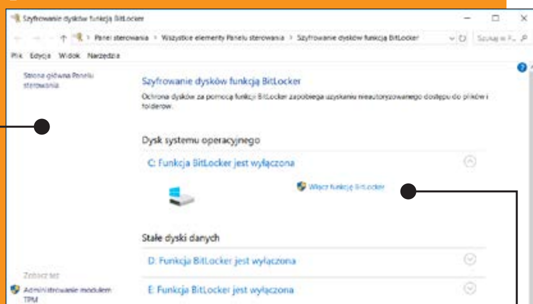


BITLOCKER CZY VERACRYPT

Jeśli korzystamy z Windows 10 w wersji Pro, Enterprise lub Education, możemy skorzystać z dostępnej systemowo opcji szyfrowania dysku **BitLocker** ●. Wykorzystuje ona moduł TPM (Trusted Platform Module). Jest to standard układu scalonego, który służy do wykonywania kryptograficznych obliczeń. Każdy układ TPM ma prywatny klucz RSA i unikatowy numer seryjny. BitLocker wykorzystuje moduł TPM do weryfikacji zaszyfrowanego dysku. Jest to bardzo bezpieczne rozwiązanie, gdyż klucz prywatny jest zawsze w komputerze, a jednocześnie nawet sam użytkownik go nie zna, nie można go również przechwycić i odczytać.

Jeśli nasze urządzenie nie ma wbudowanego modułu TPM, przy szyfrowaniu z użyciem funkcji BitLocker będzie potrzebny nam pendrive. To właśnie na nim będzie przechowywany klucz prywatny niezbędny do odszyfrowania dysku.

Do odblokowania dysku potrzebne są dwa elementy – hasło, które sami wymyślimy, i klucz prywatny, który może być w module TPM wbudowany w komputer lub na USB.



Czy nasze urządzenie ma moduł TPM

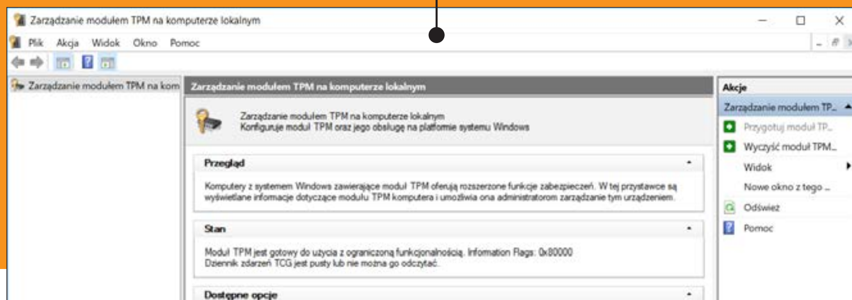
Korzystamy ze skrótu klawiaturowego [Win]+[R]. W oknie wpisujemy **tpm.msc** i klikamy na **OK**. Jeżeli nasze urządzenie jest wyposażone w moduł TPM, pojawi się okno z informacjami o układzie ●. Jeśli nie mamy takiego modułu, system wyświetli informację, że nie może odnaleźć takiego układu.

Korzystamy z BitLockera

1 W wyszukiwarkę systemową wpisujemy **BitLocker** i klikamy na znalezioną funkcję.

2 Klikamy na **Włącz funkcję BitLocker** ●, przy wybranym dysku, który chcemy zabezpieczyć. Postępujemy zgodnie z instrukcjami kreatora. Jeśli nasz komputer nie jest wyposażony w moduł TPM, musimy przygotować pendrive.

Nawet jeśli nasz Windows ma funkcję BitLocker, warto rozważyć korzystanie z programu **VeraCrypt**, który oferuje rozwiązanie podobne, ale uważane za bezpieczniejsze. BitLocker to funkcja systemowa, czyli jest możliwe, że Microsoft jest w stanie odblokować każdy zaszyfrowany zasób. VeraCrypt to otwarte oprogramowanie, które przeszło wiele audytów bezpieczeństwa i nie ma wad w kodzie. Dodatkowo pozwala na zaszyfrowanie tylko wybranej przestrzeni dysku, a nie całej jego powierzchni.



4 Następnie wybieramy opcję **Standardowy wolumen VeraCrypt** i klikamy na **Dalej**.

Typ wolumenu

Standardowy wolumen VeraCrypt

Wybierz tę opcję, aby utworzyć zwykły wolumen VeraCrypt.

Ukryty wolumen VeraCrypt

Czasem może wystąpić sytuacja, w której ktoś zmusza do ujawnienia hasła do zaszyfrowanego wolumenu. Istnieje wiele sytuacji, gdy nie można odmówić ujawnienia hasła (np. w sytuacji zagrożenia życia lub zdrowia). Użycie tzw. wolumenów ukrytych pozwala na wyjście z opresji bez ujawnienia właściwego hasła.

5 Teraz klikamy na **Wybierz plik**. Musimy podać nazwę naszego wolumenu i jego lokalizację. Nie wybierajmy istniejącego pliku, gdyż zostanie on skasowany – pliki do zaszyfrowania przenosimy do wolumenu dopiero po jego utworzeniu.

Lokalizacja wolumenu

D:\Wolumen

Wybierz plik...

Nigdy nie zapisuj historii

Wolumen VeraCrypt jest umieszczony w pliku (zwanym kontenerem/magazynem VeraCrypt), który może być umieszczony na dysku twardym lub USB itp. Magazyn VeraCrypt jest jak normalny plik (może on być, np. przeniesiony lun skasowany jak każdy normalny plik). Kliknij 'Wybierz plik' i wybierz nazwę pliku dla magazynu i wybierz lokalizację, gdzie chcesz, aby został stworzony.

Uwaga: Jeżeli wybierzesz istniejący plik, VeraCrypt NIE zaszyfruje go; plik zostanie skasowany i zastąpiony nowo tworzonym magazynem VeraCrypt. Jeżeli chcesz zaszyfrować istniejący plik (lub później) przesuń go do magazynu VeraCrypt, który teraz tworzysz.

6 Pozostawiamy ustawienia algorytmów szyfrujących i mieszania bez zmian i klikamy na **Dalej**.

Opcje szyfrowania

Algorytm szyfrowania

AES | Testuj

Zaakceptowany przez FIPS szyfr (Rijndael, opublikowany w 1998) może być używany przez agencje rządowe USA Do ochrony informacji zaklasyfikowanych jako ściśle tajne. Klucz 256-bitowy, z blokiem 128-bitowym, 14 przebiegów (AES-256). Tryb szyfrowania: XTS.

Więcej informacji na temat AES | Test wydajności

Algorytm mieszający

SHA-512 | Informacja o algorytmach

7 Teraz podajemy rozmiar wolumenu (zwróćmy uwagę na jednostki, w których podajemy dane). Po wpisaniu wartości klikamy na **Dalej**.

Wielkość wolumenu

6 | KB | MB | GB | TB

Wolne miejsce na dysku D:\ wynosi 456.19 GB

Wskaż rozmiar kontenera do utworzenia.

Jeśli tworzysz dynamiczny (sparse-file) kontener, ten parametr wskazuje maksymalny możliwy rozmiar.

Zauważ, że minimalny możliwy rozmiar woluminu FAT wynosi 292 KB. Minimalny możliwy rozmiar wolumenu exFAT to 424 KB. Minimalny możliwy rozmiar wolumenu NTFS to 3792 KB. Minimalny możliwy rozmiar wolumenu ReFS to 642 MB.

Pomoc | < Wstecz | Dalej > | Anuluj

8 Następnie podajemy hasło, które będzie chroniło nasz wolumen. Rekomendowane jest hasło o długości przynajmniej 20 znaków. Najlepiej, jeśli będzie zawierało również przynajmniej jedną dużą literę, cyfrę i znak specjalny.

Hasło wolumenu

Hasło: ••••••••••••••••••••••••••••••

Potwierdź: ••••••••••••••••••••••••••••••

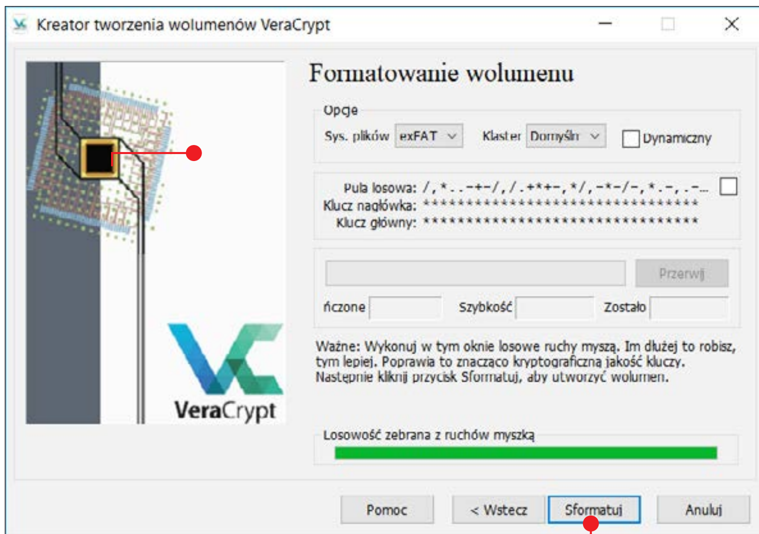
Użyj plików-kluczy | Pliki-klucze...

Wyświetl hasło

Użyj PIM

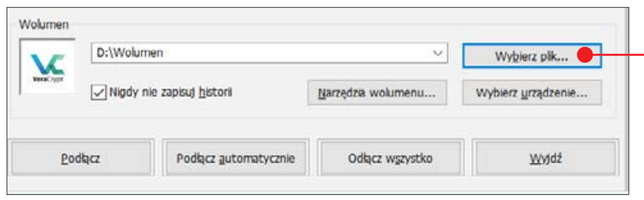
Bardzo ważne jest wybranie dobrego hasła. Powinieneś unikać wybrania pojedynczych słów, które mogą być znalezione w słowniku (lub kombinacji 2, 3, lub 4 znalezionych słów). Nie powinno zawierać, żadnych nazw, imion lub dat urodzin. Nie powinno być łatwe do wymyślenia. Dobrym hasłem jest przypadkowa kombinacja dużych i małych liter, cyfr, i znaków specjalnych, takich jak @ ^ = $ * + itp. Zalecamy wybranie hasła zawierającego więcej niż 20 znaków (dłuższe, lepsze). Maksymalna długość - 64 znaki.

9 W kolejnym kroku musimy określić, czy będziemy przechowywać pliki większe niż 4 GB. Jeśli tak, wybierzmy system plików exFAT lub NTFS. Musimy również wykonywać losowe ruchy myszą w celu poprawy kryptograficznej jakości generowanych



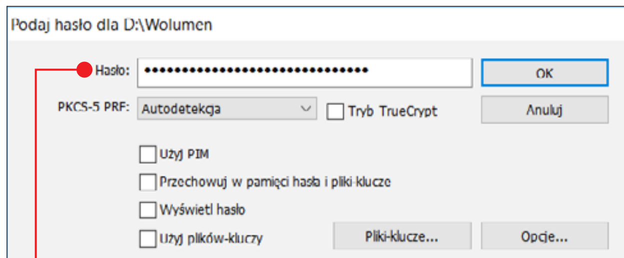
kluczy. Dopiero gdy pasek dojdzie do końca, klikamy na **Sformatuj** ●.

10 Po utworzeniu wolumenu klikamy na **Zakończ**.



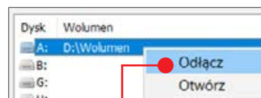
Korzystamy z wolumenu

1 W głównym oknie programu VeraCrypt klikamy na **Wybierz plik** ●. Wybieramy nasz wolumen, a następnie klikamy na **Podłącz**.



2 Podajemy hasło ● i klikamy na **OK**.

3 Po udanej weryfikacji nasz zasób zostanie dodany jako nowy dysk ● i będziemy mogli korzystać z niego w normalny sposób – kopiując, zapisując pliki itp. Po zakończeniu pracy w programie VeraCrypt klikamy na wolumen prawym przyciskiem myszy i z menu wybieramy opcję **Odłącz** ●.



Dysk lokalny (A:)	Dysk lokalny	5,99 GB	5,99 GB
Dysk lokalny (C:)	Dysk lokalny	237 GB	44,1 GB
Dysk lokalny (D:)	Dysk lokalny	1,20 TB	450 GB
Dysk lokalny (E:)	Dysk lokalny	617 GB	76,8 GB

4 Znikamy z internetu

PROGRAMY OPISANE W TYM ROZDZIALE ZNAJDZIESZ NA DVD

Często mówi się, że jeśli coś raz trafiło do internetu, pozostaje w nim już na zawsze. Oczywiście jest to prawda, jednak możemy podjąć odpowiednie kroki w celu usunięcia różnych treści z sieci – zwłaszcza takich, które dotyczą nas osobiście

Usuwanie kont w popularnych serwisach

Jeśli zależy nam na prywatności, powinniśmy skupić się w pierwszej kolejności na usunięciu lub dezaktywacji kont w serwisach społecznościowych. Zobaczmy, jak tego dokonać, na przykładzie tych, z których korzysta się najczęściej. Serwisy internetowe często zmieniają układ i wygląd menu czy ustawień, jednak opierając się na opisanych krokach, powinniśmy skutecznie usunąć lub dezaktywować konto w danym serwisie, nawet jeśli będzie nieco inaczej wyglądał.



Facebook

To najpopularniejszy serwis społecznościowy w Polsce. Możemy umieszczać na nim informacje o nas, komunikować się ze znajomymi, przesyłać pliki. Korzystając z niego, zgadzamy się między innymi na wyświetlane nam reklamy, tworzenie spersonalizowanego profilu reklamowego czy sprzedaż zebranych o nas informacji do firm trzecich.

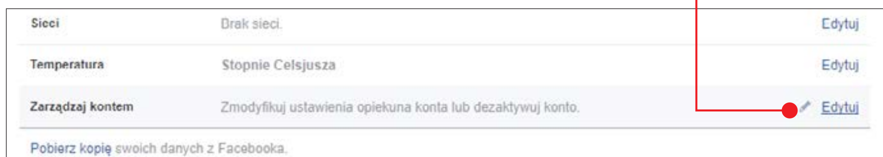
Dezaktywacja

Jest to standardowe rozwiązanie w przypadku Facebooka. Możemy dezaktywować konto, usuwając tym samym naszą nazwę profilu, imię, nazwisko oraz zdjęcia z większości udostępnianych treści. Niektóre treści nadal mogą być widoczne dla innych użytkowników serwisu.

1 Logujemy się na nasze konto Facebook, a następnie klikamy na strzałkę w górnym prawym rogu i z menu wybieramy opcję **Ustawienia**.



2 Teraz po prawej stronie klikamy na **Edytuj** przy opcji **Zarządzaj kontem**.



KONTA NA WIELU URZĄDZENIACH

Pamiętajmy, że gdy usuniemy konto w wybranym serwisie, nie będzie ono dostępne na żadnym naszym urządzeniu. Nie możemy zablokować dostępu do konta na komputerze, a korzystać z niego na smartfonie. Konto jest przypisane do serwera serwisu, a nie do naszego urządzenia.

STATUS IN MEMORIAM

Jest to specjalny status przyznawany dla konta zmarłej osoby. Konto ze statusem **In memoriam** to miejsce, w którym znajomi i rodzina mogą dzielić się ze sobą wspomnieniami o zmarłej osobie. Cechy wyróżniające konta ze statusem In memoriam to między innymi:

- Obok imienia i nazwiska na stronie profilu znajdują się słowa **In memoriam**.
- Znajomi mogą dzielić się wspomnieniami na osi czasu zmarłej osoby, jeśli zezwalają na to ustawienia prywatności konta In memoriam.
- Materiały udostępnione przez zmarłą osobę (zdjęcia, posty) pozostają na Facebooku i są widoczne dla odbiorców, którym zostały udostępnione.
- Profile ze statusem In memoriam nie pojawiają się w obszarach publicznych, takich jak propozycje osób, które możesz znać, reklamy czy przypomnienia o urodzinach.
- Nie można logować się do konta ze statusem In memoriam.
- Nie można modyfikować kont ze statusem In memoriam, do których nie przypisano opiekuna konta.

Dezaktywuj konto

Dezaktywowanie konta spowoduje wyłączenie profilu oraz usunięcie imienia, nazwiska i zdjęć z większości materiałów udostępnionych na Facebooku. Niektóre informacje mogą pozostać widoczne dla innych osób, np. Twoje imię i nazwisko na listach znajomych i wysłane wiadomości. Dowiedz się więcej.

Dezaktywuj konto.

Zamknij

3 Następnie klikamy na **Dezaktywuj konto**.

Aby kontynuować, wprowadź hasło.

Krzysiek Dziedzic

Strona, którą próbujesz odwiedzić, wymaga ponownego wpisania hasła do Twojego konta.

Hasło ••••••••••••••••

Nie pamiętasz hasła?

Kontynuuj

4 Potem musimy jeszcze raz podać hasło do naszego konta i kliknąć na **Kontynuuj**.

Przyczyna opuszczenia (wymagane)
- Chwilowo nie będę korzystać z serwisu.
- Mam zastrzeżenia dotyczące prywatności.

Pamiętaj, że zawsze masz kontrolę nad udostępnianymi przez siebie informacjami i tym, kto je może zobaczyć. Zanim dezaktywujesz konto, dowiedz się więcej... na temat ustawień prywatności na Facebooku. Jeśli masz pytania lub wątpliwości, powiadom nas, abyśmy mogli zająć się tym w przyszłości.

- Nie czuję się bezpiecznie na Facebooku.
- Nie wiem, jak korzystać z Facebooka.
- Spędzam zbyt dużo czasu na Facebooku.
- Mam inne konto na Facebooku.
- Facebook nie jest dla mnie użyteczny.
- Ktoś złamał zabezpieczenia mojego konta.
- Otrzymuję zbyt wiele wiadomości e-mail, zaproszeń i próśb z Facebooka.
- Inne (patrz dodatkowe objaśnienia):

Podaj więcej szczegółów

Rezygnacja z wiadomości e-mail: Zrezygnuj z otrzymywania w przyszłości wiadomości e-mail z Facebooka

Nawet po dezaktywacji znajomi będą mogli nadal zapraszać Cię na wydarzenia lub do grup albo oznaczać Cię na zdjęciach. Jeżeli zrezygnujesz, NIE będziesz otrzymywać takich wiadomości e-mail z zaproszeniami i powiadomieniami od znajomych.

Dezaktywacja Anuluj

5 Teraz trzeba wybrać lub podać powód dezaktywacji konta. Na koniec klikamy na **Dezaktywacja**. **Uwaga!** Przy tej metodzie zawieszenia konta możliwe jest jego przywrócenie. Wystarczy po dezaktywacji się zalogować i będziemy mogli ponownie aktywować nasze konto z wszystkimi informacjami i znajomymi.

FACEBOOK A ODEJŚCIE BLISKICH

Konta w serwisie Facebook nie są zawieszane automatycznie i teoretycznie pozostają aktywne na zawsze. Jeśli jednak ktoś z naszych bliskich odejdzie, w większości przypadków chcielibyśmy, żeby jego konto zostało usunięte lub miało status In memoriam, który jest przeznaczony dla kont osób, których już z nami nie ma. Możemy sami wystąpić z prośbą do serwisu Facebook o zmianę statusu konta bliskiej osoby lub o usunięcie takiego konta. Nie musimy mieć hasła dostępu do takiego konta.

Wniosek specjalny dotyczący konta ubezwłasnowolnionej lub zmarłej osoby

Skorzystaj z tego formularza, aby przesłać wniosek o usunięcie konta ubezwłasnowolnionej lub zmarłej osoby albo prośbę o nadanie kontu statusu In memoriam. Składamy wyrazy współczucia i prosimy o cierpliwość podczas tej procedury. Zapytania niezwiązane z powyższymi tematami mogą pozostać bez odpowiedzi. Aby chronić prywatność użytkowników Facebooka, nie możemy dostarczyć danych logowania do kont.

Twoje pełne imię i nazwisko

Krzysiek Dziedzic

Uwaga! Aby usunąć konto zmarłej osoby, należy potwierdzić, że jest się członkiem bliskiej rodziny lub wykonawcą testamentu.

Pełne imię i nazwisko właściciela konta

Jan Kowalski

Adres internetowy (URL) osi czasu tej osoby

https://www.facebook.com/jan.kowalski.5052?lst=100

Uwaga: Adres URL można znaleźć na pasku adresu przeglądarki:



Adres e-mail powiązany z kontem

Adres e-mail, który mógł zostać użyty do utworzenia konta

jan.kowalski77712@gmail.com

Jak możemy Ci pomóc?

- Nadaj temu kontu status In memoriam
- Proszę o usunięcie tego konta, ponieważ jego właściciel zmarł
- Proszę o usunięcie tego konta, ponieważ jego właściciel jest osobą ubezwłasnowolnioną
- Chcę przesłać konkretną prośbę
- Mam pytanie

Aby usunąć konto bliskiej Ci osoby, musisz dostarczyć nam skan lub zdjęcie jej świadectwa zgonu.

Jeśli nie masz świadectwa zgonu, odwiedź Centrum pomocy, aby dowiedzieć się, jakie inne typy dokumentów akceptujemy.

1 Po zalogowaniu się do naszego konta wchodzimy na adres: **https://www.facebook.com/help/contact/228813257197480**.

2 Pojawi się specjalny wniosek, który należy dokładnie wypełnić. Potrzebne do weryfikacji będą również skany dokumentów, które należy przesłać.

3 Do potwierdzenia naszych uprawnień będzie konieczne posiadanie jednego z dokumentów: pełnomocnictwo, akt urodzenia, ostatnia wola i testament, oświadczenie o powołaniu na zarządcę majątkowego. Alternatywnie nasze konto musi mieć status opiekuna zmarłej osoby.

4 W celu potwierdzenia śmierci bliskiej osoby musimy również przedstawić dokument do weryfikacji. Może być to nekrolog, karta upamiętniająca zmarłego lub akt zgonu.

5 Powinniśmy zasłonić wszelkie informacje, które nie są wymagane do weryfikacji, na przykład numer PESEL i inne tego typu dane.

6 Cała procedura jest nadzorowana przez człowieka, a nie komputer, więc rozpatrzenie i realizacja naszego wniosku nie będą natychmiastowe.

Usuwanie konta

Możemy również całkowicie usunąć konto w serwisie Facebook. Proces ten trwa bardzo długo (nawet do 90 dni) i nie ma możliwości jego odwrócenia.

1 Logujemy się na nasze konto w serwisie Facebook.

2 Następnie wchodzimy na stronę **https://www.facebook.com/help/delete_account** i klikamy na **Usuń moje konto**.

Usuń moje konto

Jeśli uważasz, że nie będziesz już korzystać ze swojego konta na Facebooku i w związku z tym chcesz je usunąć, możemy się tym zająć. Pamiętaj, że nie będziesz mógł reaktywować swojego konta ani odzyskać żadnych treści ani informacji, które się w nim znajdowały.

Jeśli nadal chcesz usunąć swoje konto, kliknij opcję „Usuń moje konto".

Dowiedz się więcej o usuwaniu konta | Usuń moje konto | Anuluj

Usuń konto na stałe

Chcesz trwale usunąć swoje konto. Czy jesteś pewien?
Jeśli tak, wypełnij poniższe:
Hasło: ••••••••••••••
Mechanizm zabezpieczający
Wpisz tekst poniżej
DME4yz
Nie możesz odczytać powyższego tekstu?
Pokaż inny tekst lub zabezpieczenie dźwiękowe captcha
Wprowadź tekst wyświetlony powyżej.
DME4yz
Dlaczego to widzę?
OK Anuluj

3 Podajemy nasze hasło, przepisujemy tekst z obrazka i klikamy na **OK**.

4 Rozpocznie się proces usuwania konta. W ciągu 14 dni mamy możliwość jego cofnięcia. Usuwanie wszystkich zdjęć i wpisów widocznych dla znajomych może potrwać jednak znacznie dłużej.

Usuń konto na stałe

Konto zostało dezaktywowane w witrynie i zostanie trwale usunięte w terminie 14 dni. Jeżeli w tym czasie zalogujesz się na konto, będziesz mieć możliwość anulowania tego procesu.
OK

5 Jeśli zmienimy zdanie, usuwanie możemy anulować, ponownie logując się na nasze konto i klikając na **Anuluj usuwanie**.

Twoje konto zostanie usunięte w dniu 29 stycznia 2018

Twoje konto oczekuje na usunięcie. Czy na pewno chcesz trwale usunąć swoje konto?
Potwierdź usunięcie Anuluj usuwanie



Twitter

Usuwanie konta z serwisu Twitter teoretycznie nie jest trudnym zadaniem. Jednak nie ma żadnej możliwości, aby usunąć je natychmiastowo. Konieczna jest dezaktywacja konta w serwisie, a następnie nielogowanie się do niego przez ponad 30 dni. Dopiero po tym okresie konto zostanie automatycznie usunięte i nie będzie można cofnąć tego procesu. Zanim to jednak nastąpi, nasze tweety będą widoczne.

Dezaktywacja i usuwanie

1 Po zalogowaniu się na nasze konto klikamy na awatar naszego profilu, a następnie na **Ustawienia i prywatność**.

Krzysiek Dziedzic
Profil
Listy
Chwile
Reklamy na Twitterze
Statystyki
Ustawienia i prywatność
Centrum Pomocy

2 Teraz po lewej stronie klikamy na **Konto**.

Konto
Prywatność i bezpieczeństwo
Hasło
Telefon komórkowy

3 Po prawej stronie przewijamy widok okna na sam dół strony i klikamy na **Dezaktywuj konto**.

Twoje archiwum Twittera
Poproś o swoje archiwum
Możesz poprosić o plik zawierający Twoje informacje, począwszy od Twojego pierwszego tweeta. Kiedy plik będzie gotowy do pobrania, wyślemy Ci link.
Zapisz zmiany
Dezaktywuj konto

4 Po zapoznaniu się z informacją dotyczącą dezaktywacji konta klikamy na **Dezaktywuj [nazwa konta]**.

Opuszczasz nas?
Czy na pewno nie chcesz tego przemyśleć? Powiedzieliśmy coś złego? Powiedz nam.

Zanim dezaktywujesz @…, musisz wiedzieć że:

- Będziemy przechowywać Twoje dane tylko przez 30 dni, a potem zostaną one usunięte permanentnie. Możesz w każdej chwili reaktywować swoje konto w ciągu tych 30 dni poprzez zalogowanie się.
- Nie musisz dezaktywować konta, żeby zmienić swoją nazwę użytkownika lub adres URL na Twitterze. Możesz to zrobić na stronie ustawień. Wszystkie @odpowiedzi i obserwujący pozostaną bez zmian.
- Jeśli chcesz użyć tej nazwy konta lub adresu e-mail z innym kontem w serwisie Twitter, zmień je przed dezaktywacją. Dopóki dane użytkownika nie zostaną bezpowrotnie usunięte, te informacje nie będą dostępne do użycia.
- Twoje konto powinno zostać usunięte z Twittera w ciągu kilku minut, ale niektóre treści mogą być widoczne na stronie twitter.com przez kilka dni po dezaktywacji.
- Nie mamy kontroli nad treścią zindeksowaną przez wyszukiwarki, takie jak Google.

Dezaktywuj @… Anuluj

5 Musimy jeszcze raz podać nasze hasło i kliknąć na **Dezaktywuj konto**.

Dezaktywuj konto

Wprowadź ponownie swoje hasło do Twittera, aby dezaktywować @

Hasło

Nie pamiętasz hasła?

Anuluj | Dezaktywuj konto

6 Konto zostanie usunięte, jeśli przez 30 dni nie będziemy się na nie logować.

Twoje konto jest aktualnie nieaktywne.

Twoje konto zostanie permanentnie usunięte w ciągu 30 dni.

Jeśli zmienisz zdanie, możesz ponownie aktywować swoje konto jeśli się zalogujesz zanim z

Kliknij tutaj aby zarejestrować nowe konto.

TWITTER A ODEJŚCIE

Możemy zgłosić prośbę o usunięcie konta osoby, która odeszła. Jest to trochę trudniejsze ze względu na brak polskojęzycznej strony z formularzem. Musimy wypełnić jej angielską wersję. Formularz jest pod adresem: **https://help.twitter.com/forms/privacy** po zaznaczeniu opcji – **I want to request the deactivation of a deceased or incapacitated person's account**.

Twitter privacy policy inqui

How can we help?
- I am requesting Twitter account information.
- I want to report an underage person's accou
- I want to request the deactivation of a decea account.
- I want to ask a question regarding privacy on

In the event of the death or incapacitation of a Twitter user, we to act on the behalf of the user to have an account deactivated. P you submit the form, we will send a confirmation email with fu



Instagram

Jest to serwis społecznościowy hostingujący zdjęcia. Został on przejęty przez Facebook w 2012 roku i od tamtej pory jest dalej rozwijany. Szybkie usunięcie konta bez wstępnej dezaktywacji jest w nim możliwe dzięki wykorzystaniu pewnej sztuczki. Jeśli planujemy nadal korzystać z tego konta w przyszłości, wystarczy zdecydować się na dezaktywację.

Dezaktywacja

1 Logujemy się na nasze konto w serwisie Instagram.

2 Następnie klikamy na ikonę profilu w górnym prawym rogu.

3 Następnie klikamy na **Edytuj profil**.

Edytuj profil

4 Teraz w dolnym prawym rogu klikamy na **Tymczasowe wyłączanie konta**.

Konto prywatne — Kiedy konto jest prywatne, Twoje zdjęcia i filmy na Instagramie mogą oglądać tylko zatwierdzeni przez Ciebie użytkownicy. Nie ma to wpływu na dotychczas obserwujące Ciebie osoby.

Propozycje podobnych kont — Dodaj swoje konto, kiedy polecasz podobne konta do obserwowania. [?]

Wyślij | Tymczasowe wyłączenie konta

5 Następnie musimy podać powód dezaktywacji konta i nasze hasło. Dopiero wtedy będziemy mogli kliknąć na **Wyłącz tymczasowo konto**.

Wyłącz tymczasowo konto

Witaj, krzysiekdziedzic111!

Zamiast usuwać konto, możesz je wyłączyć. Konto pozostanie ukryte, dopóki nie aktywujesz go ponownie, logując się na nim.

Konto można wyłączać tylko raz na tydzień.

Dlaczego wyłączasz konto? — Obawy dotyczące prywatności

Zanim wyłączysz tymczasowo konto, warto przeczytać następujące artykuły w Centrum pomocy.
- Chcę zablokować użytkownika
- Chcę mieć konto prywatne
- Chcę przestać obserwować użytkownika
- Moje konto zostało zaatakowane przez hakera

Aby kontynuować, wprowadź hasło ponownie

Po naciśnięciu poniższego przycisku Twoje zdjęcia, komentarze i polubienia zostaną ukryte, dopóki nie aktywujesz ponownie konta, logując się na nim.

Wyłącz tymczasowo konto

6 Pozostanie ono wyłączone do czasu, aż ponownie się na nie zalogujemy. Nie zostanie ono automatycznie skasowane.

Usuwanie konta na stałe

1 Powtarzamy pierwsze cztery kroki poprzedniej porady.

2 Po tym, jak zobaczymy stronę z prośbą o podanie powodu dezaktywacji konta, klikamy na pasek adresowy naszej przeglądarki i zmieniamy ostatnią część adresu.

3 Zamiast https://www.instagram.com/accounts/remove/request/temporary/ wpisujemy **https://www.instagram.com/accounts/remove/request/permanent/** i wciskamy enter.

4 Teraz wystarczy podać powód usunięcia konta i nasze hasło, a następnie kliknąć na **Usuń trwale moje konto**.

Usuń swoje konto

Witaj, [illegible]!

Przykro nam, że chcesz usunąć konto

Jeżeli niepokoją Cię zmiany naszego Regulaminu usług, wyjaśniliśmy niektóre kwestie, o które pytali użytkownicy.

Jeżeli chcesz tylko zrobić sobie przerwę, możesz zamiast tego tymczasowo wyłączyć konto na Instagramie.

Dlaczego usuwasz konto? Obawy dotyczące prywatności

Zapoznaj się z poniższymi artykułami w naszym Centrum pomocy, zanim nieodwracalnie usuniesz konto.

- Chcę zablokować użytkownika
- Chcę mieć konto prywatne
- Chcę przestać obserwować użytkownika
- Moje konto zostało zaatakowane przez hakera

Aby kontynuować, wprowadź hasło ponownie ••••••••••

Kiedy użyjesz poniższego przycisku, Twoje zdjęcia, komentarze, polubienia, znajomości oraz wszystkie inne dane zostaną nieodwracalnie usunięte. Jeżeli w przyszłości zdecydujesz się założyć nowe konto na Instagramie, nie będzie można używać tej samej nazwy użytkownika.

Usuń trwale moje konto

Usługi Google

Jest to tak naprawdę konto połączone, umożliwiające użytkownikom dostęp do wielu różnego rodzaju usług i serwisów. Korzystamy z niego, logując się na pocztę Gmail, Dysk Google, na YouTube i w wielu innych usługach.

Uwaga! W większości przypadków osoby korzystające ze smartfonów z systemem Android muszą mieć aktywne konto Google do korzystania ze sklepu Play, który zawiera aplikacje. Dodatkowo informacje o kontaktach również przechowywane są na koncie Google. Dlatego zanim zdecydujemy się na jego usunięcie, powinniśmy zabezpieczyć swoje dane lub utworzyć zapasowe konto.

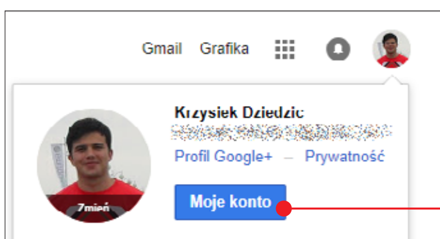
Usuwamy usługi z konta Google

1 Wchodzimy na stronę **www.google.pl**, a następnie w prawym górnym rogu klikamy na **Zaloguj się**.

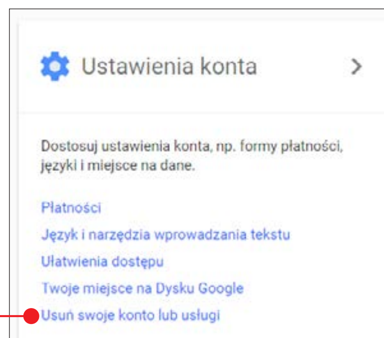


2 Podajemy dane naszego konta i logujemy się.

3 Następnie ponownie klikamy w prawym górnym rogu strony startowej Google, tym razem jednak na awatar naszego konta, a później klikamy na **Moje konto**.



4 Teraz klikamy na **Usuń swoje konto lub usługi**.



Usuń swoje konto lub usługi

Jeśli nie chcesz już używać wybranych usług Google, takich jak Gmail czy Google+, możesz je tutaj usunąć. Możesz nawet usunąć całe swoje konto Google.



Usuń usługi

Usuń konto Google i powiązane z nim dane

5 Następnie klikamy na **Usuń usługi**.

6 Podajemy hasło dostępu do naszego konta i klikamy na **Dalej**.

Krzysiek Dziedzic

Aby kontynuować, potwierdź swoją tożsamość

Wpisz hasło

Nie pamiętasz hasła? DALEJ

7 Teraz możemy usunąć wybraną usługę z naszego konta, klikając na symbol kosza przy danej opcji.

Konto Google daje dostęp do wielu usług. Niektóre z nich możesz usunąć z konta indywidualnie.

Przed usunięciem usługi rozważ pobranie z niej swoich danych.

POBIERZ DANE

Lub wybierz jedną z tych usług:

Google+
3 znajomych w 0 kręgach

YouTube
4 przesłane filmy

Gmail
8058 rozmów

8 Jeśli zdecydujemy się na usunięcie usługi Gmail, będziemy musieli podać

Jak będziesz logować się w Google

Aby dalej używać na tym koncie innych usług Google, np. Google Play, Dokumenty czy Kalendarz, potrzebujesz adresu do logowania. Nie może to być adres w Gmailu.

Wpisz adres e-mail

Wyślemy wiadomość weryfikacyjną na ten nowy adres. Nie usuniemy Gmaila z Twojego konta, dopóki nie potwierdzisz nowego adresu przez kliknięcie linku w wiadomości weryfikacyjnej.

ANULUJ WYŚLIJ WERYFIKACYJNEGO E-MAILA

inny adres e-mail, który będzie służył do weryfikacji i logowania w innych usługach, których nie można usunąć z naszego konta. Nie może być to inny adres z domeny gmail.com.

9 Dalej postępujemy zgodnie z instrukcjami.

Usuwamy konto Google

1 Powtarzamy pierwsze cztery kroki poprzedniej porady i klikamy na **Usuń konto Google i powiązane z nim dane**.

2 Podajemy hasło do naszego konta i klikamy na **Dalej**.

Krzysiek Dziedzic

Aby kontynuować, potwierdź swoją tożsamość

Wpisz hasło

Nie pamiętasz hasła? DALEJ

Wszystkie te treści zostaną usunięte

Uwaga: lista poniżej może nie zawierać wszystkich usług Google objętych usunięciem, np. tych, których Google już nie obsługuje. Dane z tych usług również zostaną usunięte.

Gmail — 149 wątków zostanie usuniętych

Ostatnia: Top Trades – Currency Pairs *12 stycznia, 04:42*

Jeśli masz oczekujące na realizację transakcje finansowe, nadal ponosisz odpowiedzialność za ewentualne należności z ich tytułu.

☑ Przyjmuję do wiadomości, że nadal odpowiadam za wszelkie obciążenia wynikające z wszystkich oczekujących transakcji finansowych, i zdaję sobie sprawę, że w określonych warunkach moje zarobki nie zostaną wypłacone.

☑ Tak, chcę trwale usunąć to konto Google i wszystkie znajdujące się na nim dane.

USUŃ KONTO   ANULUJ

3 Teraz możemy sprawdzić, jakie dane zostaną usunięte wraz z naszym kontem. Następnie musimy zaznaczyć obydwie opcje, potwierdzając, że chcemy trwale usunąć konto i bierzemy odpowiedzialność za wszelkie zobowiązania, jakimi obciążone jest konto, i na koniec klikamy na **Usuń konto**.

4 Jeśli usunęliśmy konto przez przypadek, możemy przez krótki czas je przywrócić, stosując się do instrukcji, które znajdziemy pod linkiem **Pomoc dotycząca konta**.

Twoje konto Google i wszystkie związane z nim dane

Jeśli Twoje konto Google zostało usunięte przez pomyłkę, przez krótki czas możesz spróbować je odzyskać:

1. Otwórz stronę Pomoc dotycząca konta
2. Wykonaj te czynności, by potwierdzić, że to jest Twoje konto

ZAPOMNIANE PRZEZ NAS KONTA I SERWISY

Często jest tak, że przez wiele lat, korzystając z komputera i internetu, zakładamy konta w wielu witrynach, forach, serwisach. O części z nich pamiętamy, jeśli korzystamy z nich regularnie. Jednak o wielu zapominamy, nie potrzebujemy ich używać. Tymczasem takie często przypadkowo założone konta nadal pozostają w sieci i można odnaleźć je, korzystając z wyszukiwarki. Powinniśmy usuwać niepotrzebne konta, zwłaszcza jeśli korzystamy z podobnych lub takich samych haseł w wielu serwisach. Może się zdarzyć, że ktoś uzyska dostęp do bazy danych haseł mało popularnego portalu i pozna nasze hasło, którego używamy także w innych usługach.

1 Najprostszym sposobem jest wpisanie naszego najczęściej wykorzystywanego aliasu, nazwy konta czy innej charakterystycznej cechy zakładanych przez nas kont wprost do wyszukiwarki Google.

2 Dzięki temu szybko odnajdziemy konta, których jeszcze nie skasowaliśmy, i takie, o których zapomnieliśmy.

3 Wchodzimy na odnalezione konta i usuwamy je podobnie jak w wypadku opisanych popularnych serwisów.

Agnieszka | Profil zawodowy - LinkedIn
https://pl.linkedin.com/in/agnieszka 1a457845
Warszawa, woj. mazowieckie, Polska - Redaktor - Ringer Axel Springer
Wyświetl profil użytkownika Agnieszka na LinkedIn, największej sieci zawodowej na świecie. Doświadczenie użytkownika Agnieszka zawiera Ringer Axel Springer, Wydawnictwo MT Biznes i Wydawnictwo Poltext Sp. z o.o.. Agnieszka studiował(a) na uczelni Uniwersytet Warszawski.

Wyzwania HR » Autor:
www.wyzwaniahr.pl/author/agnieszka /
Agnieszka . Redaktorka „od zawsze" i z zamiłowania – w wydawnictwach książkowych i prasowych, żyje, żeby czytać i czyta, by żyć. Od lat związana z miesięcznikiem „Komputer Świat", prowadzi serię książek i magazynów poradnikowych. A równolegle w wydawnictwach MT Biznes, Poltext i Laurum redaguje ...

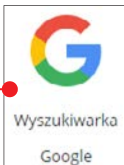
Usuwanie informacji z Google

Może się zdarzyć, że jakieś treści zostały umieszczone w internecie bez naszej zgody i stawiają nas w złym świetle lub ktoś uzyskał nasze poufne dane i rozpowszechnia je w sieci. W takiej sytuacji powinniśmy natychmiast zareagować. Przede wszystkim, jeśli uważamy, że mogło zostać popełnione przestępstwo, powinniśmy udać się na policję w celu odnalezienia osoby, która rozpowszechnia szkodliwe treści. W następnej kolejności możemy zwrócić się do Google o ich usunięcie.

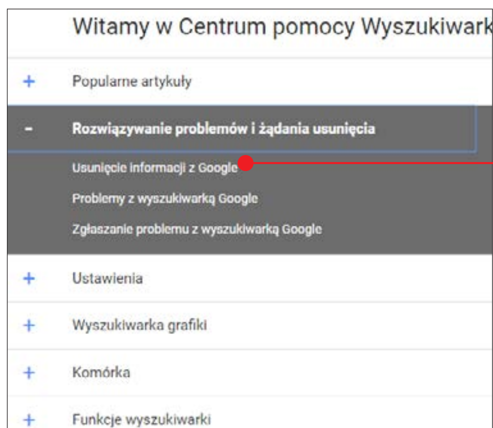
Szukamy informacji o usuwaniu danych

1 Proces usuwania treści z serwisu Google zależy od samej treści, którą chcemy usunąć, dlatego ważne jest, aby zapoznać się z polityką firmy.

2 Wchodzimy na stronę **www.google.support.com** i klikamy na **Wyszukiwarka Google**.



3 Następnie klikamy na kategorię **Rozwiązywanie problemów i żądania usunięcia**, a następnie na **Usunięcie informacji z Google**.



Usunięcie informacji z Google

Możesz zwrócić się do nas z prośbą usunięcie z wyników wyszukiwania Google in rachunku bankowego czy obrazu przedstawiającego Twój odręczny podpis).

Jakie informacje są usuwane przez Google

Zapoznaj się z naszymi Zasadami usuwania treści, by dowiedzieć się, jakie info

Jeśli chcesz usunąć zdjęcie, link do profilu lub stronę internetową z wyników wysz skontaktować z właścicielem strony (webmasterem) i poprosić go o usunięcie tyc

4 Zanim przejdziemy do zgłaszania treści, powinniśmy kliknąć na link przenoszący do **Zasad usuwania treści**.

5 Dowiemy się na tej stronie, jakie informacje podlegają zgłoszeniu i zostaną uwzględnione. Jeśli sprawa dotyczy numeru telefonu osoby nieletniej, jest szansa na jego usunięcie z zasobów serwera, pomimo że zazwyczaj tego typu dane nie są usuwane.

Usunięcie ze względów prawnych

Z wyników wyszukiwania usuwamy treści, które zawierają:

- Materiały wizualne związane z wykorzystywaniem seksualnym dzieci.
- Możemy też usuwać je w odpowiedzi na właściwe wnioski prawne takie jak zawiadomieni autorskich zgodne z ustawą Digital Millennium Copyright Act.

Dane osobowe

Z wyników wyszukiwania Google możemy usuwać niektóre rodzaje poufnych danych osobow

Informacje, które możemy usunąć

Informacje, które możemy usunąć

- krajowe numery identyfikacyjne – takie jak amerykański numer ubezpieczenia społec indywidualny numer identyfikacji podatkowej, brazylijski Cadastro de pessoas Física rejestracyjny obywatela, chińska karta identyfikacyjna obywatela itd.;
- numery kont bankowych;
- numery kart kredytowych;
- zdjęcia podpisów;
- zdjęcia prezentujące nagość lub mające charakter jednoznacznie seksualny, które zo udostępnione bez zgody przedstawionych osób;
- poufne, osobiste dane medyczne osób prywatnych.

Informacje, których zazwyczaj nie usuwamy

- data urodzenia,
- adresy,
- numery telefonów.

W jaki sposób określamy, czy usunąć dane osobowe

Prośba o usunięcie danych osobowych

Zgłoszenie usunięcia z wyników wyszukiwania

Składając wniosek o usunięcie danych do Google, musimy mieć świadomość, że informacje, które pokazuje wyszukiwarka, są znajdowane najczęściej na stronach, które nie należą do firmy Google i nie może ona brać za nie odpowiedzialności – Google odpowiada jedynie za wyniki wyszukiwania. Jeśli więc nawet nasza prośba o usunięcie z wyników wyszukiwania zostanie rozpatrzona pozytywnie, nadal będzie można uzyskać dostęp do danej treści nie przez wyszukiwarkę, ale bezpośrednio na stronach, na których występuje – wystarczy znać ich adres lub skorzystać z innej wyszukiwarki, na przykład Bing.

1 Wykonujemy pierwsze trzy kroki poprzedniej porady i przewijamy widok okna do pola **Co chcesz zrobić?**

2 Zaznaczamy opcję **Usuwanie informacji wyświetlanych w wyszukiwarce Google**.

Co chcesz zrobić?
Usuwanie informacji wyświetlanych w wyszukiwarce Google
Zapobieganie wyświetlaniu informacji w wynikach wyszukiwania Google

3 Następnie wybieramy opcję **W wynikach wyszukiwania i na stronie internetowej**.

Wskaż, gdzie widzisz informacje, które chcesz usunąć.
Informacje, które chcę usunąć, są:
W wynikach wyszukiwania Google i na stronie internetowej
Tylko w wynikach wyszukiwania Google

4 Teraz będziemy musieli podać konkretnie, jakie dane chcemy zgłosić. Zaznaczamy kolejne odpowiedzi, aż dojdziemy do ostatniej opcji.
W zdecydowanej większości przypadków wszystko zależeć będzie od naszego kontaktu z webmasterem danej strony internetowej, która udostępnia nasze dane.

Informacje, które chcę usunąć, są: W wynikach wyszukiwania Google i na stronie internetowej
Kontaktowałeś się z nim?
Nie, nie chcę tego robić ze względu na charakter przedstawionych informacji
Chcę usunąć Dokument lub numer identyfikacyjny nadany przez instytucję rządową
Wybierz kraj, w którym wydano dokument/nadano numer: Polska
Wybierz typ pokazywanego dokumentu lub numeru identyfikacyjnego: PESEL lub numer ubezpieczenia społecznego

Jeśli na stronie podanej w wynikach wyszukiwania Google znajduje się Twój numer PESEL lub numer dokumentu tożsamości, najpierw skontaktuj się z właścicielem lub webmasterem strony i poproś o usunięcie tych danych. Dzięki temu informacje zostaną całkowicie usunięte.

Jeśli Twoje dane osobowe nadal pojawiają się na opublikowanej stronie i w wynikach wyszukiwania Google, prześlij nam informacje wskazane poniżej, a my zbadamy sprawę.

Jeśli Twoja prośba o usunięcie nie pasuje do tej kategorii, wróć do narzędzia do zgłaszania próśb o usunięcie strony internetowej i wybierz odpowiedni rodzaj usunięcia.

Twoje imię i nazwisko *

Kontaktowałeś się z nim?

Chcę, by informacje o mnie zostały usunięte zgodnie z europejskim prawem o ochronie danych.

Jeśli chcesz poprosić Google o usunięcie treści z wyników wyszukiwania zgodnie z europejskim prawem o ochronie danych, wejdź na stronę usuwania treści ze względów prawnych .

Europejskie prawo o ochronie danych

Możemy skorzystać z tego prawa – pozwoli nam na usunięcie wybranych wyników wyszukiwania, które wskazują na naszą osobę, nieważne, czy będą to ogólnie dostępne informacje, czy też nie.

1 Zaznaczamy kolejno opcje: **Usuwanie informacji wyświetlanych w wyszukiwarce Google**, **W wynikach wyszukiwania i na stronie internetowej**, **Chcę, by informacje o mnie zostały usunięte zgodnie z europejskim prawem o ochronie danych**, a następnie klikamy na link .

2 Teraz wybieramy opcję dotyczącą **prawa do bycia zapomnianym** i klikamy na odpowiedni link u dołu strony .

Proszę wybrać spośród następujących opcji Chcę zgłosić prośbę o usunięcie z listy informacji zgodnie z przepisami europejskiego prawa w zakresie ochrony danych (prawo do bycia zapomnianym)

Nawet jeśli usuniemy objętą zgłoszeniem witrynę z wyników wyszukiwania Google, będzie ona w dalszym ciągu istnieć i będzie można znaleźć ją bezpośrednio (używając jej URL-a) lub za pomocą innych wyszukiwarek. Indeks Google tak naprawdę wskazuje tylko, że strona istnieje w internecie, a nie, że Google ją poleca. Dlatego najlepszym rozwiązaniem jest skontaktowanie się z webmasterem, który może całkowicie usunąć stronę.

Jeśli uważasz, że treść, którą należy usunąć, ma charakter zniesławiający, kliknij tutaj, jeśli nie, przejdź tutaj.

3 Dopiero teraz będziemy mogli wypełnić bardzo szczegółowy i rozbudowany formularz , który pozwoli na w miarę szybkie usunięcie danych z wyszukiwarki na nasz temat.

Usunięcie danych osobowych zgodnie z przepisami UE

Prośba o usunięcie treści zindeksowanej przez wyszukiwarkę Google

Trybunał Sprawiedliwości Unii Europejskiej w orzeczeniu z maja 2014 roku (C-131/12 z 13 maja 2014 r.) stw
osób ma priorytet nad prawem dostępu do tych wyników.

Po otrzymaniu takiej prośby oceniamy potrzebę ochrony prywatności danej osoby, jednocześnie biorąc pod
publiczne zainteresowanie tymi informacjami; możemy na przykład odmówić usunięcia informacji na temat

Do wypełnienia tego formularza potrzebna jest cyfrowa kopia dokumentu potwierdzającego Twoją tożsamoś

* Pole wymagane

TWOJE DANE

Kraj prawa właściwego dla Twojej prośby *
Wybierz kraj/region ▾

4 Google będzie weryfikował każde zgłoszenie i o decyzji zostaniemy powiadomieni drogą mailową.

Kontakt z webmasterem

Usuwanie danych z samej wyszukiwarki na niewiele może nam się zdać, jeśli treść nadal będzie udostępniana na konkretnej witrynie. Koniecznie musimy skontaktować się z administratorem strony i wystąpić do niego z prośbą o usunięcie danej treści. Nie należy niczego wymagać, a jedynie zwrócić się z prośbą, ponieważ bez sądowego wyroku właściciel strony nie musi niczego zmieniać, może jedynie z uprzejmości, rozumiejąc nasze racje, zgodzić się na nasz wniosek. Piszmy prośby w języku danej strony. Jeśli witryna jest angielska, nie piszmy prośby po polsku.

Sposoby na kontakt:

- **Skontaktuj się z nami lub Kontakt** – szukamy na stronie internetowej informacji o kontakcie, gdzie przeważnie powinien być

O Komputerswiat.pl | Kontakt | Regulamin i polityka prywatności | Cookies | Reklama | Statystyki | Usługi IT

podany adres e-mail służący do kontaktu w różnych sprawach. Możemy na niego wysłać naszą prośbę.

■ **Szukanie z funkcją Whois** – możemy wykorzystać funkcjonalność wyszukiwarki Google i wpisać polecenie **whois [adres strony]** i wyszukać właściciela witryny lub adres e-mail w zakładce **Registrant Contact**. Niestety, informacje zawarte na tej stronie nie zawsze są aktualne.

■ Często najłatwiej jest **dotrzeć do firmy hostującej**, która zapewnia adres danej stronie. Możemy skontaktować się z nią, żeby ona z kolei skontaktowała się z właścicielem witryny.

WHOIS Record for Komputerswiat.p

WHOIS History | WHOIS Research | Similar Domains | Reverse IP Address

Updated 2 seconds ago

Registrant Contact

Email:

PODGLĄDAMY WYGWIAZDKOWANE HASŁA

Wielu użytkowników korzysta z automatycznego uzupełniania haseł w swoich przeglądarkach, przez co czasami sami zapominają, jakie konkretnie hasło było przypisane do jakiej witryny. Takie rozwiązanie niesie ze sobą również duże ryzyko dla naszego bezpieczeństwa, gdyż ktoś obcy po przechwyceniu naszego sprzętu mógłby bez problemu zalogować się do naszych usług. Jeśli zapomnimy naszego hasła, a jest ono dla nas dostępne w zagwiazdkowanej formie, możemy je szybko podejrzeć.

1 Otwieramy przeglądarkę Google Chrome i otwieramy stronę logowania z uzupełnionym hasłem.

Wpisz hasło

••••••••••••••••

Nie pamiętasz h

Pokaż wszystkie zapisane hasła

Wytnij Ctrl+X
Kopiuj Ctrl+C
Wklej Ctrl+V
Wklej jako zwykły tekst Ctrl+Shift+V
Zaznacz wszystko Ctrl+A
Sprawdzanie pisowni
Kierunek pisania
Save current session
Zbadaj Ctrl+Shift+I

2 Klikamy na hasło prawym przyciskiem myszy i wybieramy opcję **Zbadaj**.

3 Pojawi się ekran z kodem strony z zaznaczonym elementem odpowiadającym za pole z wpisanym hasłem. Od-

```
<div class="Xb9hP">
  <input type="password"
  "current-password" spell
```

najdujemy parametr **type="password"**, zmieniamy na **type="text"** i wciskamy enter.

```
  <input type="text" c
  password" spellcheck
```

4 Teraz po lewej stronie zauważymy, że wcześniej zakodowane hasło jest łatwe do odczytania. Dzięki temu szybko sprawdzimy nasze hasła, jeśli je zapomnimy.

Aby kontynuować, potwierdź swoją tożsamość

Wpisz hasło

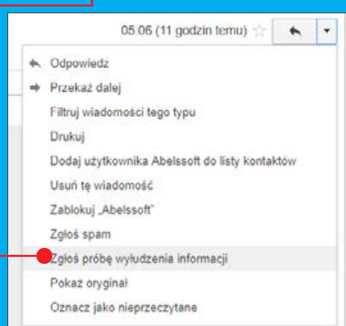
MojeUkryteHasloJestWidoczne

Nie pamiętasz hasła? DALEJ

WYŁUDZANIE INFORMACJI A GMAIL

Możemy bardzo łatwo zgłaszać ataki typu phishing, które mają na celu wyłudzenie informacji od użytkownika.

1 Korzystając z poczty Gmail, możemy zgłosić każdą wiadomość, która ma wyłudzić od nas informacje. Wystarczy otworzyć taką wiadomość, a następnie kliknąć na strzałkę w prawym górnym rogu i wybrać opcję **Zgłoś próbę wyłudzenia informacji**.



Zgłaszanie niewiarygodnego nadawcy

Phishing to forma oszustwa, w której nadawca wiadomości próbuje skłonić odbiorcę do ujawnienia ważnych informacji osobistych (takich jak hasło albo numer konta bankowego), przekazania pieniędzy lub zainstalowania szkodliwego oprogramowania. Zazwyczaj nadawca podszywa się pod przedstawiciela faktycznie istniejącej firmy lub instytucji. Więcej informacji

Jeśli uważasz, że ta wiadomość stanowi atak typu phishing, możesz zgłosić to do naszego zespołu ds. naruszeń, aby pomóc nam uniemożliwić ten i podobne ataki. Zgłoszenie tej wiadomości jako ataku spowoduje przesłanie całej wiadomości do sprawdzenia przez nasz zespół.

Zgłoś wiadomość od niewiarygodnego nadawcy | Anuluj

2 Następnie klikamy na **Zgłoś wiadomość od niewiarygodnego nadawcy**.

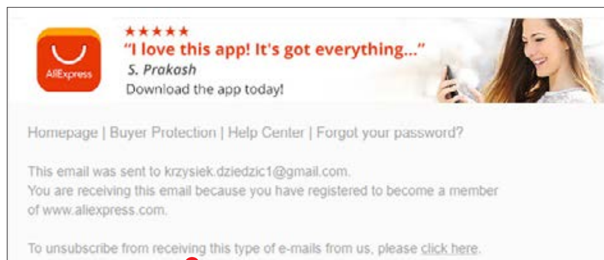
Rezygnujemy z newsletterów

Praktycznie przy każdej okazji w większości różnych stron, sklepów itp. oferowane nam są newslettery, czyli informacje handlowe, rabatowe, reklamowe, przesyłane na podany adres e-mail. Czasami nawet nieświadomie wyrażamy zgodę na otrzymywanie takich wiadomości i później nasza skrzynka pocztowa jest zasypywana przez wiele e-maili, które właściwie można traktować jak spam, na który jednak się zgodziliśmy. Z każdego takiego newslettera można zrezygnować.

1 Logujemy się na naszą skrzynkę pocztową.

2 Następnie otwieramy przykładową wiadomość zawierającą treść reklamową.





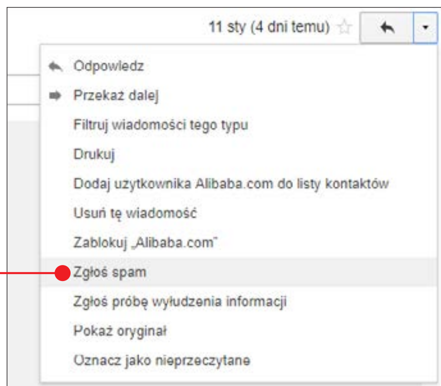
3 Teraz przeszukujemy treść wiadomości, aż znajdziemy link do kliknięcia, który pozwala na zrezygnowanie z usługi newslettera. W przypadku angielskich komunikatów najczęściej znajdziemy frazę: **To unsubscribe from receiving this type of e-mails from us, please click here**.

4 Jeśli w mailu reklamowym nie możemy znaleźć informacji o wypisaniu się z usługi, możemy odwiedzić stronę internetową, która przesłała nam tę informację. Jeżeli mamy na niej zarejestrowane konto, możemy się zalogować i sprawdzić w ustawieniach konta, czy możemy wyłączyć treści reklamowe. Jeśli takiej opcji nie ma lub nie zakładaliśmy nawet konta na danej witrynie, musimy zaznaczyć wiadomość jako spam.

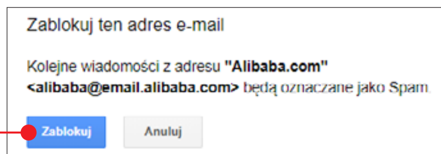
Zgłaszamy niepożądane wiadomości

1 W przypadku skrzynki pocztowej Gmail logujemy się na nasze konto.

2 Otwieramy wiadomość, którą uważamy za niepożądaną, a następnie musimy kliknąć na strzałkę w prawym górnym rogu i wybrać opcję **Zgłoś spam**.



3 Możemy również wybrać opcję **Zablokuj [Przykładowa Witryna]**. Dzięki temu po potwierdzeniu kliknięciem na **Zablokuj** wszystkie wiadomości od tego nadawcy będą automatycznie lądowały w naszym folderze **Spam**.



USUWAMY DANE Z BAZ DANYCH OPERATORÓW KOMÓRKOWYCH

Często nieświadomie wyrażamy zgodę dla operatorów komórkowych na wykorzystywanie naszych danych osobowych w celach reklamowych przy rejestracji numeru. Z punktu widzenia prywatności jest to niewskazane. Dodatkowo operatorzy mogą również udostępniać nasze dane w celach marketingowych firmom trzecim. Powinniśmy sprawdzić ustawienia zgód marketingowych na naszych kontach. Najprościej jest sprawdzić takie ustawienia bezpośrednio na stronie naszego operatora po zalogowaniu na nasze konto. Niezależnie od sieci, w której jesteśmy zarejestrowani, każdy operator musi umożliwiać zmianę tych ustawień. Tego typu zgody znajdziemy, przechodząc na przykład do zakładki **Konto i formalności**, **Zgody marketingowe**.

Uwaga! Czasem operatorzy oferują jakieś specjalne promocje w zamian za wyrażenie zgody marketingowej. Jeśli wycofamy taką zgodę, najprawdobniej oferta promocyjna zostanie dla nas wycofana.

Zgody marketingowe

Zarządzanie zgodami umożliwia podgląd jak również zmianę stanu poszczególnych zgód.

Zgody marketingowe dla konta (zwiń)

Treść zgody	Stan zgody	Operacja
Nie znaleziono żadnych dostępnych zgód dla konta		

Zgody marketingowe dla telefonu (zwiń)

Treść zgody	Stan zgody	Operacja
1.Wyrażam zgodę na otrzymywanie informacji handlowych drogą elektroniczną. Zgoda jest niezależna od czasu obowiązywania Umowy.	Dozwolone	Wycofaj zgodę
2.Wyrażam zgodę na przetwarzanie danych transmisyjnych dla celów marketingu usług telekomunikacyjnych w trakcie trwania Umowy.	Dozwolone	Wycofaj zgodę
3.Wyrażam zgodę na używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego. Zgoda jest niezależna od czasu obowiązywania Umowy.	Dozwolone	Wycofaj zgodę
4.Wyrażam zgodę na przetwarzanie adresu do korespondencji, numeru telefonu oraz adresu e-mail w celach marketingowych podmiotów trzecich. Zgoda jest niezależna od czasu obowiązywania Umowy.	Dozwolone	Wycofaj zgodę
5.Wyrażam zgodę na przetwarzanie adresu e-mail i telefonu kontaktowego, danych zawartych w kopiach dokumentów przez POLKOMTEL (a) w celu podjęcia działań		

PROGRAMY OPISANE W TYM ROZDZIALE ZNAJDZIESZ **NA DVD**

5 Serwisy społecznościowe i banki: dyskretnie i bezpiecznie

Serwisy społecznościowe pomagają utrzymywać kontakty prywatne i służbowe – pod warunkiem że korzystamy z nich w odpowiednio bezpieczny i dyskretny sposób. Podobnie strony banków ogromnie ułatwiają życie i można używać ich bez obaw – także pod pewnymi warunkami. Przeczytajmy, jak bez ryzyka posługiwać się ważnymi usługami online

Anonimowość a serwisy społecznościowe

Serwisy społecznościowe nie zapewniają praktycznie żadnej anonimowości. Warto więc wiedzieć, jak najbezpieczniej z nich korzystać oraz jak skonfigurować nasze konta na Facebooku, Twitterze, Instagramie i konto Google tak, by chronić prywatność. Ważne, aby podczas korzystania z tych serwisów pamiętać, że tak naprawdę jeśli coś raz trafi do internetu – to w nim zostaje. Dlatego zawsze udostępniajmy tylko przemyślane treści.

USTAWIENIA A AKTUALIZACJE

Serwisy społecznościowe często są aktualizowane, zdarza się nawet, że dla różnych użytkowników są wprowadzane inne zmiany.
Dlatego może się zdarzyć, że czynności przedstawione w poradach w tym rozdziale będą za jakiś czas wyglądały nieco inaczej. Generalnie jednak kluczowe funkcje powinny działać tak, jak zostało to opisane.
Zawsze warto również krok po kroku samemu przeanalizować wszystkie dostępne ustawienia – być może sami odkryjemy takie, które w naszym wypadku warto zmienić, bo zagrażają naszej prywatności i bezpieczeństwu.

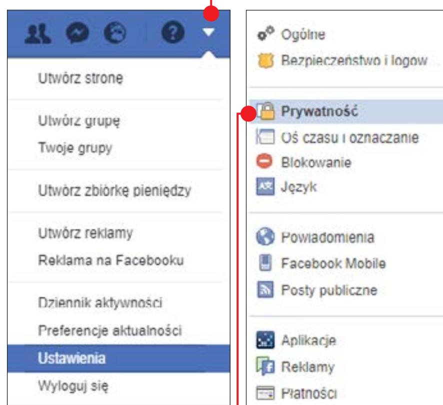


Facebook

Po założeniu konta domyślnie odblokowanych jest wiele opcji, które mogą być niepożądane, jeżeli zależy nam na zachowaniu prywatności. Na przykład według domyślnych ustawień zdjęcia umieszczane przez nas w naszej galerii są widoczne dla wszystkich, którzy odwiedzą nasz profil. Jeśli nasz profil i zdjęcia są prywatne, lepiej ograniczyć możliwość oglądania fotografii i zapewnić to tylko znajomym lub wybranym osobom.

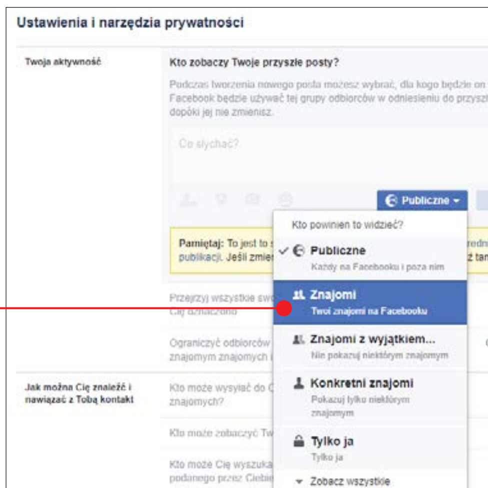
Ustawienia prywatności

1 Po zalogowaniu do konta Facebook klikamy na strzałkę w prawym górnym rogu, a następnie na **Ustawienia**.

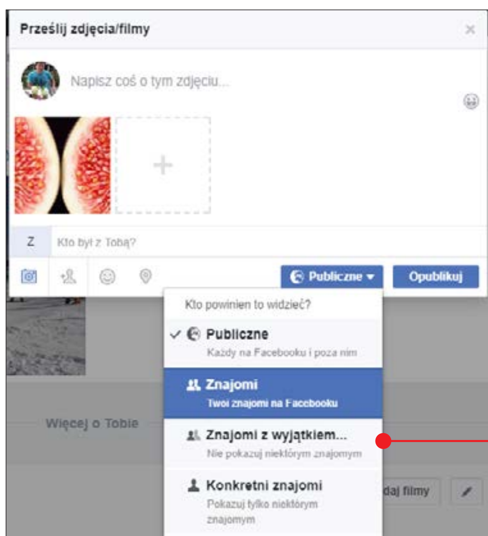


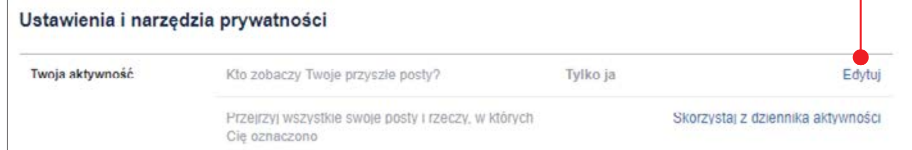
2 Teraz po lewej stronie klikamy na **Prywatność**.

3 Po prawej stronie w linii **Twoja aktywność** klikamy na **Edytuj**. Wystarczy zmienić domyślne ustawienia z **Publiczne** na **Znajomi** lub **Konkretni znajomi**.



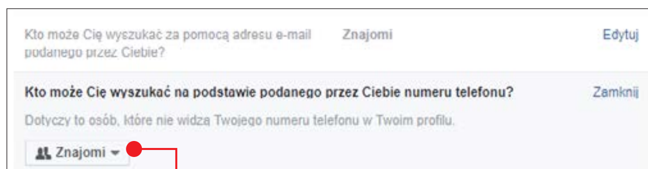
4 Możemy również modyfikować widoczność jednego zdjęcia czy posta w trakcie jego publikacji, co może być przydatne w konkretnych sytuacjach.





Ukrywamy listę znajomych i nie tylko

1 Wykonujemy pierwsze dwa kroki poprzedniej porady, następnie po prawej stronie ekranu klikamy w dziale **Jak można Cię znaleźć i nawiązać z Tobą kontakt** na **Kto może zobaczyć Twoją listę znajomych?** i zmieniamy ustawienia na **Tylko ja**. Dzięki



temu obcy nie będą mogli sprawdzać, kogo „mamy w znajomych".

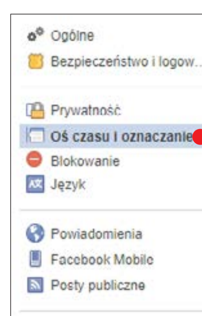
2 Warto również zmienić ustawienia wyszukiwania za pomocą adresu e-mail i numeru telefonu na **Znajomi** zamiast **Publiczne**. Ograniczy to możliwość nieznanym nam osobom na wyszukanie naszego profilu.

Weryfikacja oznaczenia

Czasem dla żartu lub przez złośliwość różne osoby mogą chcieć oznaczyć nas na zdjęciu, które nam się nie podoba lub jest kompromitujące. Jeśli włączymy weryfikację oznaczeń, będziemy mogli temu zapobiec, a dodatkowo bardzo szybko będziemy mogli poprosić serwis o całkowite usunięcie danego zdjęcia.

1 Po zalogowaniu do konta Facebook klikamy na strzałkę w prawym górnym rogu, a potem na **Ustawienia**.

2 Następnie po lewej stronie klikamy na **Oś czasu i oznaczanie**.





3 Teraz po prawej stronie klikamy na pierwszą pozycję w polu **Weryfikacja** i włączamy opcję, która umożliwi nam kontrolę oznaczania zdjęć z naszym udziałem.

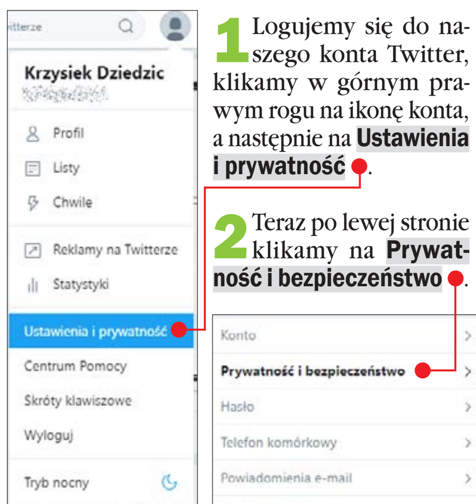


Twitter

Działanie tego serwisu polega na rozpowszechnianiu postów – tweetów. Nie zawsze jednak może być nam na rękę całkowicie publiczne postowanie jakichś informacji, na przykład takich, które dotyczą tylko konkretnej grupy znajomych lub osób zainteresowanych danym tematem. Dlatego też warto przejrzeć ustawienia prywatności w tym serwisie i skonfigurować je tak, by odpowiadały naszym potrzebom.

Prywatne tweety

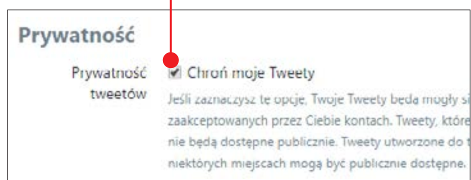
Ta opcja pozwoli nam na kontrolowanie, na jakich kontach będą wyświetlane nasze tweety.



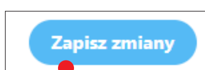
1 Logujemy się do naszego konta Twitter, klikamy w górnym prawym rogu na ikonę konta, a następnie na **Ustawienia i prywatność**.

2 Teraz po lewej stronie klikamy na **Prywatność i bezpieczeństwo**.

3 Po prawej stronie pojawi się okno, w którym musimy włączyć funkcję **Chroń moje Tweety**.



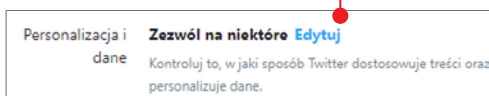
4 Pamiętajmy, że aby zmiany zostały zastosowane, musimy na dole strony kliknąć na **Zapisz zmiany**.



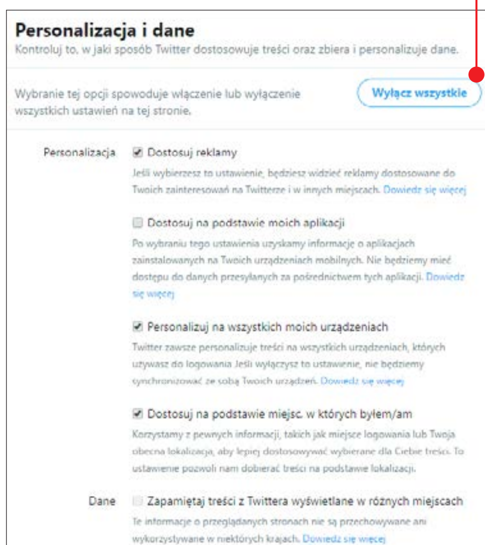
Wyłączamy zbieranie danych

Twitter podobnie jak inne serwisy zbiera o nas informacje i na tej podstawie wyświetla reklamy, przekazuje również informacje o nas do firm trzecich.

1 Jeśli chcemy wyłączyć takie działanie serwisu, wykonujemy dwa pierwsze kroki poprzedniej porady, a następnie po lewej stronie ekranu klikamy na **Edytuj** przy polu **Personalizacja i dane**.



2 Teraz możemy zapoznać się szczegółowo ze wszystkimi opcjami, najszybciej wyłączymy je wszystkie, klikając na **Wyłącz wszystkie**.

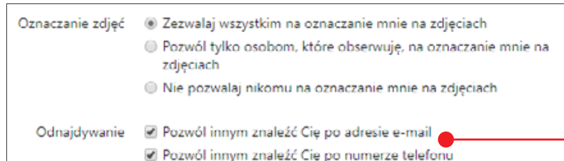


Odnajdywanie i oznaczanie

Domyślnie każdy może nas odnaleźć na Twitterze po wpisaniu w wyszukiwarkę adresu e-mail lub numeru telefonu, każdy też może nas oznaczyć w poście lub na zdjęciu – oto jak zmienić te ustawienia.

1 Przechodzimy do ustawień **Prywatność i bezpieczeństwo** (patrz poprzednia strona) naszego konta Twitter.

2 Następnie w polu **Oznaczanie zdjęć** wybieramy opcję **Nie pozwalaj nikomu na oznaczanie mnie na zdjęciach**, a w polu **Odnajdywanie** usuwamy zaznaczenia obu opcji.





3 Następnie musimy potwierdzić naszą decyzję, klikając na **Na pewno** i na koniec na **Zapisz zmiany**.

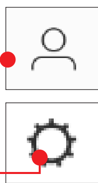


Instagram

Korzystanie z serwisu Instagram jest bardzo wygodne i proste, jednak domyślne ustawienia nie zapewniają prywatności. Dodane przez nas zdjęcie może od razu zobaczyć każdy – lepiej to zmienić. Warto też włączyć opcję cenzurowania komentarzy, aby pod naszymi zdjęciami nie mogły pojawiać się nieodpowiadające nam treści.

Konto prywatne

1 Logujemy się do serwisu i klikamy na ikonę konta, a potem wchodzimy w opcje (jeśli korzystamy z Instagrama na komputerze w oknie przeglądarki czy w aplikacji, klikamy na , a na smartfonie naciskamy trzy kropki w prawym górnym rogu ekranu).



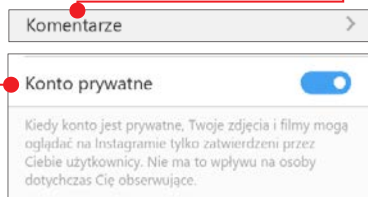
2 Odnajdujemy opcję **Konto prywatne** i włączamy ją. Gotowe. Od teraz tylko zatwierdzone przez nas osoby będą mogły oglądać zdjęcia z naszego profilu.

OCHRONA PRYWATNOŚCI

Informacje o innych ustawieniach dotyczących ochrony prywatności znajdziemy w Centrum pomocy Instagramu (w opcjach aplikacji mobilnej lub po kliknięciu na Prywatność u dołu strony serwisu online oraz na help.instagram.com).

Cenzura komentarzy

1 Powtarzamy krok **1** z poprzedniej wskazówki i klikamy na **Komentarze**.



2 Włączamy opcję **Ukryj niestosowne komentarze**. Możemy sami dodawać słowa klucze, które będą powodowały automatyczne usuwanie komentarzy.





Google

Ustawienia prywatności w przypadku konta Google są dość skomplikowane, ponieważ mogą dotyczyć wielu urządzeń oraz wielu usług, jak Gmail, Hangouts, YouTube, Chrome, Mapy Google i inne. Poznajmy domyślne ustawienia Google, które w największym stopniu narażają naszą prywatność i anonimowość.

Anonimowość w Google

Są usługi i funkcje, które nie pozwalają na bycie anonimowym, bo jest to sprzeczne z ich przeznaczeniem, dotyczy to na przykład Map Google, choćby dodanie zdjęcia do map musi być zweryfikowane kontem Google, a bez włączenia lokalizacji nie da się korzystać z nawigacji. Jedynym sposobem, żeby to obejść, jest stworzenie specjalnego konta, z którego będziemy korzystać, gdy nie będziemy chcieli, by jakieś dane zostały przypisane do nas.



Warto również korzystać z sesji **Incognito** w przeglądarce Chrome i nie logować się do konta Google – wtedy historia przeglądania nie będzie zapisywana na naszym koncie.

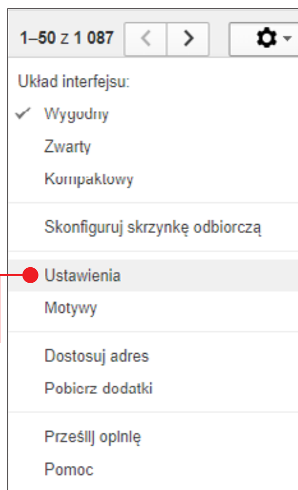
Gmail i Hangouts

W tych usługach nie będziemy mieli zbyt wielu zmian do wprowadzenia. Jednak warto się im przyjrzeć.



Zdjęcie i wyświetlanie obrazów

W usłudze Gmail domyślnie zdjęcie przypisane do naszego profilu Google+ jest wyświetlane dla wszystkich osób. Możemy łatwo to zmienić.



1 Logujemy się do naszego konta Gmail, a następnie klikamy na ikonę ustawień w prawym górnym rogu i na **Ustawienia**.

2 Teraz w nowym oknie odnajdujemy pozycję **Moje zdjęcie** i zmieniamy opcję na **Widoczne tylko dla osób, z którymi mogę czatować**.

3 Warto też zmienić opcję automatycznego wyświetlania obrazów w e-mailach w polu **Obrazy**. Dzięki temu na przykład będziemy mogli zdecydować, by nie pobierać grafik, gdy korzystamy z publicznych punktów dostępu, a także wtedy, gdy nasz monitor jest dobrze widoczny dla innych.

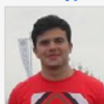


Aktywność w Hangouts

Domyślnie jesteśmy widoczni dla wszystkich osób, które mamy dodane do listy znajomych w Hangouts. Widzą one, czy jesteśmy online i z jakiego urządzenia korzystamy (smartfona czy komputera). Możemy jednak się ukryć.

Obrazy:
- Zawsze wyświetlaj obrazy zewnętrzne - Dowiedz się więcej
- Pytaj przed wyświetleniem obrazów zewnętrznych

Moje zdjęcie:
Dowiedz się więcej
Zmień zdjęcie

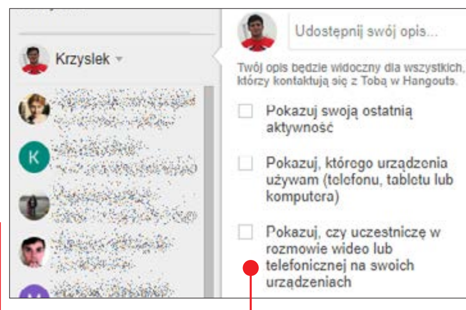


- Widoczne dla każdego
- Widoczne tylko dla osób, z którymi mogę czatować

Jeśli masz zdjęcie w profilu Google, jest ono zawsze widoczne dla wszystkich.

1 Po zalogowaniu do konta Gmail w oknie poczty klikamy na ikonę naszego profilu Hangouts.

2 Pojawi się okno z ustawieniami. Usuwamy zaznaczenia przy pierwszych trzech opcjach dotyczących ostatniej aktywności, używanego urządzenia oraz prowadzonych rozmów – to zapewni nam większą anonimowość.



REKLAMY NA KONCIE GOOGLE I NIE TYLKO

Klikając na ikonę naszego konta Google, na **Moje konto** i w sekcji **Dane osobowe i prywatność** na **Ustawienia reklam**, możemy zarządzać ustawieniami reklam. Możemy zdecydować o wyłączeniu opcji **Personalizacja reklam** – to ustawienie pozwala Google na korzystanie z informacji o naszej aktywności na koncie i informacji przechowywanych w usługach Google (takich jak wyszukiwarka i YouTube), by wyświetlać dopasowane do nas reklamy na wszystkich urządzeniach, na których się logujemy, oraz we wszystkich usługach Google. Możemy tu też zmienić tematy reklam, które nas interesują. Warto też zapoznać się z serwisem **Your Online Choices** (**www.youronlinechoices.com/pl/twojewybory),** który pozwala na wyłączanie reklam behawioralnych (opartych na wyszukiwaniu) od wybranych dostawców współpracujących z wydawcami stron przy zbieraniu i przetwarzaniu informacji. Aby dowiedzieć się więcej o danym dostawcy, klikamy na strzałkę w kolumnie **Info** przy jego nazwie.



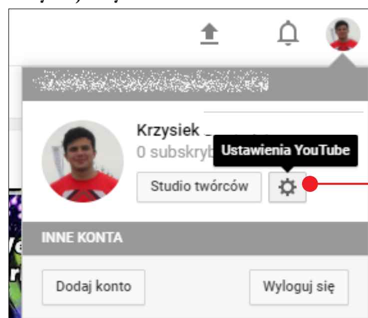




Firma	Włączona/Wyłączona	Status	Info
1plusX	Wł. Wył.		
33Across	Wł. Wył.		
4W MARKETPLACE SRL	Spróbuj połączyć ponownie		
Accordant Media	Spróbuj połączyć ponownie		
ad4mat	Wł. Wył.		



Możemy ukryć przed innymi to, jakie filmy polubiliśmy lub jakich twórców subskrybujemy.



1 Logujemy się na nasze konto YouTube, klikamy na ikonę naszego profilu w prawym górnym rogu, a potem na **Ustawienia YouTube**.

USTAWIENIA KONTA
Ogólne
Połączone konta
Prywatność
Powiadomienia
Odtwarzanie
Połączone telewizory

2 Następnie po lewej stronie klikamy na **Prywatność**.

3 W tej zakładce możemy wyłączyć domyślne ustawienia, które sprawiają, że wszyscy widzą, jakie filmy polubiliśmy lub dodaliśmy do publicznej playlisty. Jeśli chcemy zachować maksymalną anonimowość, możemy zaznaczyć wszystkie opcje w oknie **Fajne i subskrypcje** i usunąć zaznaczenia wszystkich opcji w oknie **Obszar aktywności**.

Prywatność
Fajne i subskrypcje
Chcę, aby polubione przeze mnie filmy były prywatne
Nie ujawniaj zapisanych przez mnie playlist
Zachowaj moje subskrypcje jako prywatne
Obszar aktywności
Zdecyduj, czy informacje o Twoich publicznych działaniach mają się pojawia… prywatnych filmów, nie będą tam wyświetlane. Komunikaty ze strumienia m… internetowych.
Publikuj informacje w moim strumieniu aktywności, gdy...
Dodam film do publicznej playlisty
Spodoba mi się film
Zapiszę playlistę
Zasubskrybuję kanał
Zapisz

4 Na koniec zatwierdzamy zmiany, klikając na **Zapisz**.

KONTA NA SMARTFONIE

Warto pamiętać, że większość serwisów społecznościowych ma osobne ustawienia na smartfonie i na komputerze. Nawet jeśli wyłączymy jakąś opcję na pecece, może okazać się, że na urządzeniu mobilnym nadal pozostało stare ustawienie i treści umieszczane przez nas są widoczne nie w taki sposób, jak się spodziewamy. Dlatego koniecznie trzeba sprawdzać wszelkie opcje prywatności i bezpieczeństwa na obu rodzajach urządzeń.
Jeśli przez przypadek pozwolimy grze mobilnej na umieszczanie wpisów w serwisach społecznościowych, automatycznie będą dodawane w naszym imieniu posty za każdym razem, gdy przejdziemy poziom lub zdobędziemy osiągnięcie, dlatego najlepiej wyłączyć takie powiadomienia. W wypadku urządzeń z Androidem odpowiednie ustawienia znajdziemy w aplikacji Gry Google Play.

Ustawienia
Publiczny profil gracza
Loguj się w grach automatycznie
Zezwalaj Grom Play na automatyczne logowanie się do gier
Używaj tego konta do logowania
We wszystkich nowych grach
Możliwość wykrycia profilu gracza
Zezwól innym na odnalezienie Twojego ID gracza na podstawie nazwiska lub adresu e-mail w Google
Włącz wibracje dla powiadomień
Tylko ważne powiadomienia
Powiadomienia multiplayer
Pozwalaj grom wysyłać powiadomienia o rozgrywkach wieloosobowych
Powiadomienia o zadaniach
Pozwalaj grom wysyłać powiadomienia o zadaniach
Powiadomienia o prośbach
Pozwalaj grom wysyłać powiadomienia o prezentach i zaproszeniach

Bezpieczne korzystanie z banków internetowych

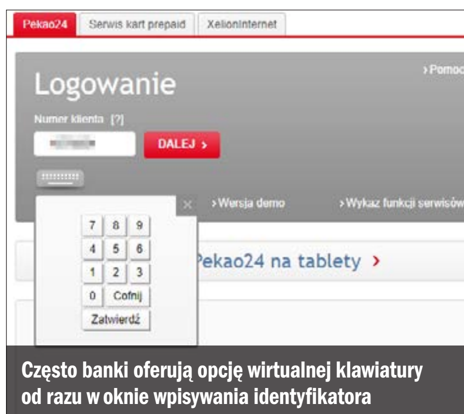
Niezwykle ważne jest bezpieczne korzystanie z bankowości internetowej. Coraz więcej osób przekonuje się do tej formy obsługi swoich rachunków, istnieją nawet banki całkowicie mobilne, które nie mają fizycznych oddziałów. Korzystanie z tego typu rozwiązań jest bardzo wygodne i z reguły bezpieczne, ponieważ większość banków ma zabezpieczenia na wysokim poziomie. Przyjrzyjmy się bliżej, jak przebiega korzystanie z bankowości online.

Przelew bankowy

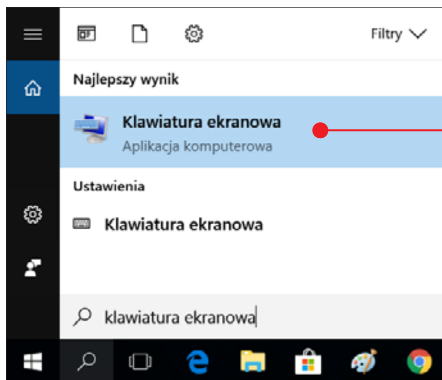
Załóżmy, że chcemy wykonać przelew bankowy. Po pierwsze, musimy zalogować się na nasze konto. Wchodzimy na stronę banku. Pierwsze, na co powinniśmy zwrócić uwagę, to **wygląd strony banku** – czy nie odbiega on od normy. Trzeba też również upewnić się, że **połączenie z bankiem jest szyfrowane**. Poinformuje nas o tym **ikona kłódki** na pasku przeglądarki i początek adresu **HTTPS**. Następnie podajemy **dane logowania**, czyli nasz numer identyfikacyjny i hasło. Ten proces może się różnić w zależności od banku – może się na niego składać więcej sposobów weryfikacji naszej tożsamości.

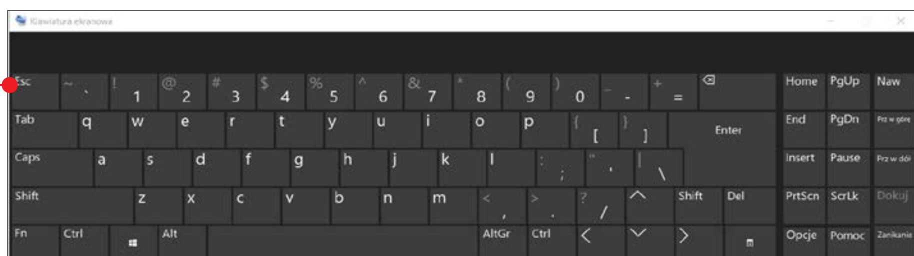
Najlepiej korzystać z **klawiatury ekranowej**, ponieważ jeśli na naszym urządzeniu jest keylogger (złośliwy program, który przechwytuje wszystkie wciśnięte klawisze z klawiatury), atakujący może poznać nasze dane. Taką klawiaturę uruchamiamy w Windows, wpisując w wyszukiwarkę systemową **Klawiatura ekranowa** i klikając na znalezioną pozycję.

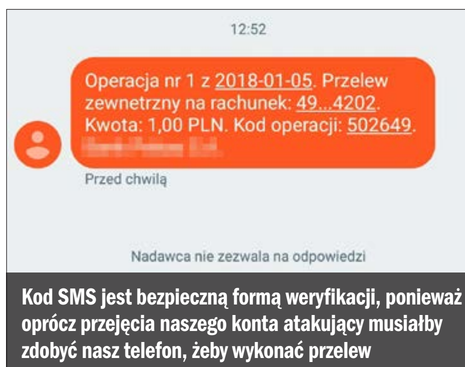
Teraz przechodzimy do odpowiedniej zakładki do wykonania przelewu, podajemy wszystkie



Często banki oferują opcję wirtualnej klawiatury od razu w oknie wpisywania identyfikatora

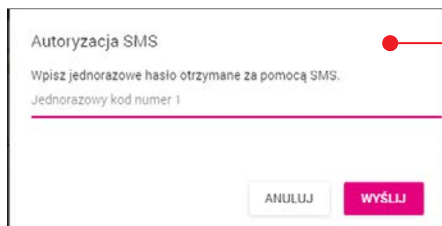






Kod SMS jest bezpieczną formą weryfikacji, ponieważ oprócz przejęcia naszego konta atakujący musiałby zdobyć nasz telefon, żeby wykonać przelew

dane i wykonujemy przelew. W zdecydowanej większości przypadków, jeśli odbiorca jest już wcześniej zdefiniowany jako stały, przelew przejdzie bez żadnych dalszych weryfikacji. Jest to wygodne, ale jednocześnie potencjalnie niebezpieczne. Najlepiej jest **zabezpieczać wykonanie przelewu SMS-em z hasłem** lub wykorzystując fizyczny **token**, jeśli bank daje taką możliwość – wtedy nawet jeśli niepowołana osoba zaloguje się na nasze konto, nie będzie mogła wykorzystać naszych środków.





Kodem SMS są zabezpieczane także płatności kartą kredytową przez internet

Karta kredytowa/debetowa

Nawet jeśli atakujący zdobędzie dostęp do naszego konta bankowego online, nasze karty i tak są bezpieczne. Włamywacz nie zobaczy wszystkich cyfr identyfikujących kartę, a co najważniejsze numer **CVC2**, który stanowi zabezpieczenie podczas zatwierdzenia płatności kartą przez internet w zależności od banku, albo w ogóle nie jest widoczny, albo jest zablokowany i żeby uzyskać do niego dostęp, musimy pobrać kod SMS lub podać token.

Dodatkowe zabezpieczenia

W zależności od banku poprawa bezpieczeństwa logowania lub weryfikacja płatności może wyglądać różnie, najlepiej skontaktować się z obsługą banku i zapytać o to, jak uzyskać najwyższe bezpieczeństwo. Przykładem dodatkowego zabezpieczenia może być dostępne w T-Mobile Usługi Bankowe logowanie dwustopniowe z wykorzystaniem skomplikowanego i długiego hasła oraz logowania wymagającego weryfikacji telefonem i specjalną aplikacją mobilną.

HOTSPOTY I PUBLICZNE OTWARTE SIECI

Jeśli chcemy skorzystać z bankowości internetowej i nie mamy dostępu do zaufanej sieci, najlepiej skorzystać z połączenia poprzez VPN (pamiętajmy tylko, że niektóre banki mogą blokować połączenie, jeśli na przykład w ciągu godziny będziemy logować się z kilku krajów). Jak tego dokonać, przeczytamy w kolejnym rozdziale. Nie możemy ryzykować łączenia się z bankiem poprzez zwykłą przeglądarkę w publicznych sieciach – istnieje ryzyko, że cały ruch jest rozszyfrowywany i przechwytywany przez osobę trzecią (atak MitM – Man in the Middle).



Fot. Paisan Homhuan/123rf.com

Poprawiamy zwykłą przeglądarkę

Korzystając z popularnych przeglądarek jak Chrome czy Firefox, nie jesteśmy anonimowi. Nawet jeśli sporadycznie używamy trybu prywatnego, potem i tak przy logowaniu się w normalnym trybie nasze dane są zapisywane na wielu stronach, a pliki cookie i inne wykonywalne skrypty mogą w czasie rzeczywistym pobierać dane o naszym urządzeniu. Na szczęście możemy sami zadbać o zwiększenie anonimowości oraz o bezpieczeństwo w popularnych przeglądarkach dzięki możliwości instalacji i konfiguracji specjalnych dodatków i rozszerzeń.

UWAGA!

Wskazówki zostały przygotowane na przykładzie przeglądarki Google Chrome, jednak możemy je wykorzystać także w innych przeglądarkach, jeśli obsługują one opisane dodatki.

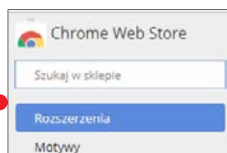
Instalowanie dodatków w Google Chrome

1 Po uruchomieniu przeglądarki Chrome klikamy na trzy kropki w prawym górnym rogu, a następnie na **Więcej narzędzi**, **Rozszerzenia**.

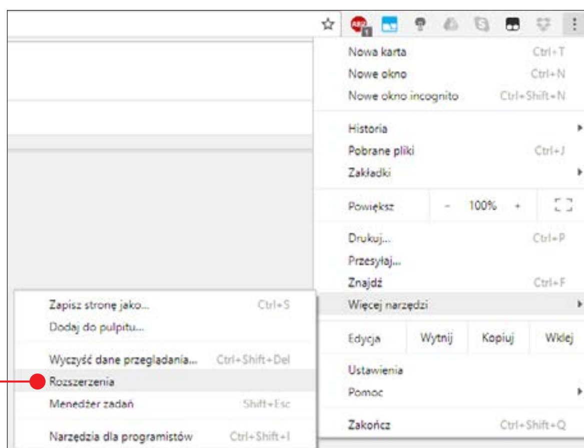
2 Na tej stronie możemy zarządzać zainstalowanymi dodatkami, włączać je i usuwać. Jeśli chcemy dodać nowe, przewijamy je na sam dół strony i klikamy na **Pobierz więcej rozszerzeń**.



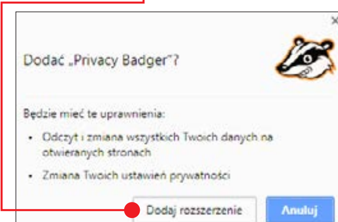
3 Następnie wystarczy podać nazwę rozszerzenia i wyszukać je.



4 Kolejnym krokiem jest kliknięcie po prawej stronie opisu rozszerzenia na **Dodaj do Chrome**.



5 Pozostaje nam tylko potwierdzić decyzje, klikając na **Dodaj rozszerzenie**.



6 Czynności te powtarzamy dla każdego rozszerzenia. Możemy również kliknąć na samo rozszerzenie, jeśli chcemy poznać szczegółowe informacje i sposób działania.

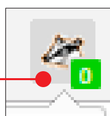




Privacy Badger

Jest to wyjątkowe narzędzie, które zapewnia ochronę przed śledzeniem nas w sieci przez firmy, które wykorzystują różnego typu identyfikatory śledzące i pliki cookies. Jego głównym zadaniem jest analiza reklam i wykrywanie tych, które chcą nas śledzić czy zapisywać nasz ruch online. Program będzie sam kontrolował domeny i pokazywał potencjalne zagrożenia, ale ostateczną decyzję, co z nimi zrobić, może podejmować użytkownik. Możemy pozwolić na wyświetlanie reklam, zablokować pliki cookie lub całkowicie zablokować domenę wyświetlającą reklamy.

Warto zapoznać się z samouczkiem dostępnym po kliknięciu na ikonę dodatku na pasku przeglądarki, a następnie na **Więcej informacji o tym jak Privacy Badger chroni Twoją prywatność**.





Przy pierwszym użyciu tego rozszerzenia zobaczymy, że mimo iż program wykrywa wiele trackerów reklamowych, żadnego z nich nie blokuje. Dopiero po przejrzeniu kilku witryn w tym samym oknie zacznie podejmować kroki w celu wyeliminowania dostawców reklam, którzy mogą stanowić zagrożenie dla naszej anonimowości.

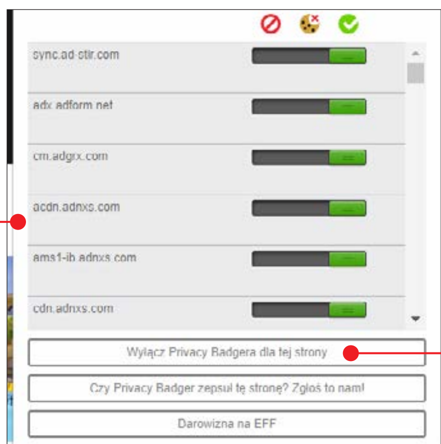
Po kilku minutach przeglądania witryn będziemy mogli zweryfikować pracę dodatku, który sam zablokuje niebezpieczne trackery. Algorytm sprawdzający usługodawców jest bardzo dobrze dopracowany i w żaden sposób nie powinien wpływać na komfort przeglądania witryn ani też na wyświetlanie bezpiecznych reklam, które akceptujemy.

Jeśli jakaś strona przestanie być poprawnie wyświetlana lub w ogóle nie będzie chciała się wyświetlić, będziemy musieli kliknąć na opcję **Wyłącz Privacy Badgera dla tej strony**. Dodatkowo również warto kliknąć na



WAŻNE

W wartościowych serwisach, które lubimy, nie blokujmy reklam, bo dzięki nim możemy mieć darmowy dostęp do ciekawych treści, które nie powstają przecież za darmo.



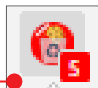


Czy Privacy Badger zepsuł tę stronę? Zgłoś to nam! – w ten sposób pomożemy deweloperom w jeszcze lepszym rozwinięciu tego rozszerzenia.
Jest to unikalne rozszerzenie, które uczy się w czasie, gdy przeglądamy różne witryny, i blokuje tylko szpiegujących dostawców reklam i złośliwe trackery. Nie blokuje natomiast reklam, które nam nie szkodzą. Dzięki temu nadal możemy wspierać twórców, którzy utrzymują serwisy internetowe z reklam, a jednocześnie pozostajemy bardziej anonimowi.



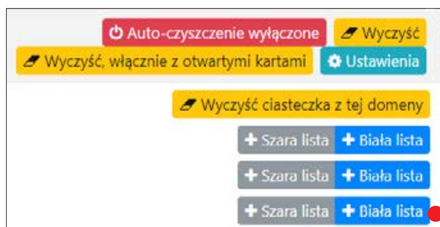
CookieAutoDelete

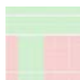
To rozszerzenie zapewnia ochronę przed śledzeniem przez pliki cookie, które przechowują w formie tekstowej informacje na nasz temat i sprawiają, że jesteśmy rozpoznawani przez odwiedzane przez nas strony.
W większości przypadków pliki cookie są bezpieczne i nie stwarzają zagrożenia. Jeśli jednak nasz komputer zostanie zaatakowany, atakujący, wykradając pliki cookie, może uzyskać dostęp do witryn, z których korzystamy, wykorzystując mechanizm działania tego typu plików. Dlatego z jednej strony dla zachowania anonimowości, a z drugiej dla zachowania bezpieczeństwa – najlepszym, choć niekoniecznie najwygodniejszym na co dzień wyjściem jest korzystanie z tego dodatku, który pozwala na automatyczne kasowanie plików cookie po zamknięciu każdej witryny. Obsługa tego rozszerzenia jest bardzo prosta.



1 Klikamy na pasku przeglądarki na ikonę tego dodatku ●.

2 Następnie klikamy na **Auto-czyszczenie wyłączone** w celu uruchomienia tej funkcji. Jeśli zależy nam na zachowaniu ciasteczek ze stron, z których często korzystamy, i ich pozostawienie według nas nie będzie stwarzać ryzyka, możemy dodać wybrane domeny do białej listy poprzez kliknięcie na **Biała lista** ● przy ich nazwach.





uMatrix

Jest to bardzo ważne rozszerzenie, które pozwala na blokowanie skryptów wykonywalnych na odwiedzanych stronach. W wypadku innych przeglądarek niż Chrome możemy zastosować rozszerzenie **No Script**, które spełnia podobną funkcję. uMatrix jest jednak znacznie bardziej zaawansowanym narzędziem, które pozwala blokować bardzo różne elementy na każdej odwiedzanej stronie i dynamicznie nimi zarządzać poprzez wygodny i przejrzysty interfejs graficzny ●.

uMatrix 1.2.0

www.imdb.com * 35 2 1

wszystko	ciastko	CSS	obraze	media	skrypt	XHR	ramka	inne
ta domena								
imdb.com	5							
www.imdb.com	1				1			
google.pl	17							
www.google.pl	3							1
images-amazon.com								
ecx.images-amazon.com					1			
media-imdb.com								
ia.media-imdb.com		2	7		7		3	1
sl-images-amazon.com								
ssl-images-amazon.com			42		1			
amazon-adsystem.com								
.amazon-adsystem.com							1	

Chodzi o skrypty typu JS (JavaScript), które mogą być uruchamiane automatycznie na stronach internetowych bez wiedzy użytkownika, co jeśli nie ma on odpowiedniej ochrony, może prowadzić do zainfekowania komputera lub wykradnięcia danych użytkownika.
Skrypty blokujemy, klikając na dolną, czerwoną część prostokąta z nazwą **Skrypt**.
Oprócz tego dodatek domyślnie czyści historię podręczną przeglądarki co 60 minut. Można wyłączyć tę funkcję, wchodząc w opcje rozszerzenia i klikając na ikonę trybu w górnym lewym rogu, a następnie usuwając zaznaczenie w zakładce **Ustawienia**, w polu **Prywatność**.

Prywatność

- Usuń zablokowane ciasteczka.
- Usuń nie zablokowane ciasteczka sesyjne 60 minut od ostatniego użycia.
- Usuwaj zawartość local storage ustawioną przez zablokowane hosty
- ✔ Wyczyść pamięć podręczną przeglądarki co 60 minut.
- ✔ Fałszuj nagłówek HTTP referer dla domen zewnętrznych.
- Ścisły HTTPS: blokuj mieszaną zawartość.
- ✔ Blokuj wszystkie próby audytowania linków [ang.].

Ważną ze względu na bezpieczeństwo funkcją uMatrixa jest również modyfikowanie pliku **hosts**, czyli swoistej czarnej listy dostępu systemu Windows. Dołączone do tej listy zostaje ponad 79 000 adresów, które mogą stanowić zagrożenie lub są kojarzone ze szkodliwym kodem.



HTTPS Everywhere

To rozszerzenie pozwala na znaczne poprawienie naszego bezpieczeństwa w sieci i jednocześnie anonimowości. Wymusza połączenie typu HTTPS zamiast standardowego HTTP. Różnica jest ogromna, ponieważ standard HTTP nie zapewnia ochrony dla przesyłanych pakietów danych. W przypadku przechwycenia osoby trzecie mogą bez żadnego kłopotu odczytać takie pakiety i wydobyć z nich na przykład hasła lub pliki cookie. Standard HTTPS zapewnia szyfrowane połączenie, pakiety przechwycone z takiego połączenia nie dadzą atakującemu praktycznie nic. Dlatego bardzo ważne jest wymuszanie tego typu połączeń.
Po kliknięciu na ikonę dodatku wystarczy upewnić się, że opcja **Włącz HTTPS Everywhere** jest aktywna.
Czasem może zdarzyć się, że jakaś witryna nie wyświetla się poprawnie, możemy wtedy wyłączyć dla niej ten dodatek. Warto pamiętać, że nie wszystkie witryny obsługują szyfrowany protokół – niektóre oferują tylko zwykły rodzaj połączenia.
Dodatek pozwala na tworzenie własnych reguł, jeśli te utworzone automatycznie nie będą działały.

uMatrix | Ustawienia | Moje reguły | Pliki hosts | O rozszerzeniu

Wszystkie nazwy hostów z plików hosts są traktowane jako czarno-listowane globalnie

Zastosuj zmiany | Aktualizuj teraz | Przeczyść całą pamięć podręczną

- Automatycznie aktualizuj pliki hosts.

79 133 blokowanych unikalnych hostów z:

- ✔ Dan Pollock's hosts file użytych 9 492 z 13 169
- ✔ hpHosts' Ad and tracking servers użytych 43 644 z 47 811
- ✔ Malware Domain List użytych 1 488 z 1 488
- ✔ Malware domains użytych 9 545 z 9 612
- ✔ MVPS HOSTS użytych 12 539 z 13 017
- ✔ Peter Lowe's Ad and tracking server list użytych 2 425 z 2 425

HTTPS Everywhere

- ✔ Włącz HTTPS Everywhere
- Blokuj wszystkie nieszyfrowane próby połączenia

Dodaj nową regułę dla tej strony

Wyświetl wszystkie reguły

O HTTPS Everywhere

Wspomóż finansowo EFF

[Wersja: 2017.12.6]

6 Tor i VPN: incognito w internecie

PROGRAMY OPISANE W TYM ROZDZIALE ZNAJDZIESZ NA DVD

W tym rozdziale przeczytamy, jak w praktyce zachować anonimowość, korzystając z internetu. Dowiemy się wszystkiego o sieci Tor, połączeniach typu VPN, szyfrowaniu e-maili oraz innych rodzajach szyfrowanej komunikacji. Porady zamieszczone na kolejnych stronach są skierowane do użytkowników, którzy zamierzają korzystać głównie z systemu Windows

Korzystamy z dwóch przeglądarek

W wypadku korzystania z internetu na komputerze, dla bezpieczeństwa i zachowania poufności bardzo ważne jest, byśmy używali **dwóch przeglądarek**. Nazwijmy je – **bezpieczna** i **zwyczajna**.
Ta pierwsza będzie służyła nam do zapewnienia anonimowości. Zawsze, gdy będziemy chcieli wykonać zadanie, które wymaga dyskrecji – choćby odwiedzić stronę internetową czy dodać na niej wpis, zachowując przy tym anonimowość, powinniśmy skorzystać z przeglądarki, która ukryje naszą obecność w sieci.
A ta druga, zwyczajna przeglądarka, będzie nam służyła, gdy będziemy normalnie przeglądać internet oraz używać serwisów społecznościowych i innych usług – zawsze wtedy, gdy możliwość rozpoznania nas po adresie IP nie będzie stanowić problemu i gdy nie zależy nam na anonimowości.

Pamiętajmy o tym, aby nigdy nie używać przeglądarek obu typów jednocześnie.

Uwaga! Mniej wygodną stroną dbania o anonimowość jest znacznie wolniejsze działanie przeglądarki bezpiecznej, która oparta jest na specjalnych mechanizmach realnie wpływających na szybkość ładowania witryn.

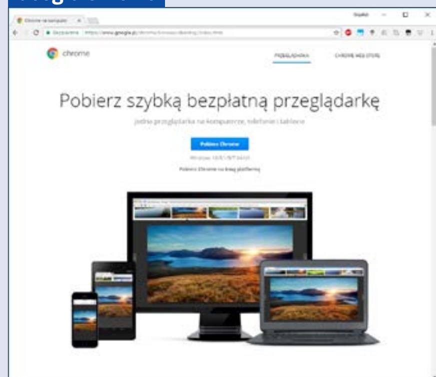
Czym jest sieć Tor i jak działa

Tor to sieć anonimowa, która podobnie jak inne sieci tego typu, czyli **Freenet**, **GNUnet** czy **MUTE**, ma za zadanie chronić naszą tożsamość w internecie. Głównym celem wykorzystywania takich sieci jest chęć ominięcia narzędzi cenzury, mechanizmów

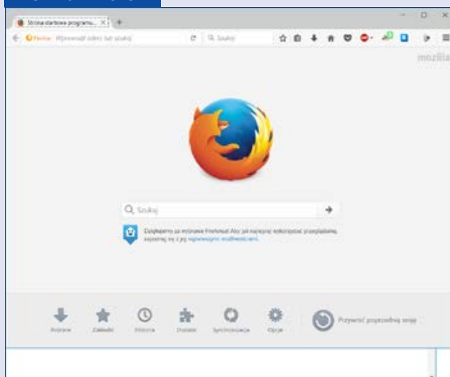
Zwyczajna przeglądarka

Tę rolę może pełnić dowolna przeglądarka, jak na przykład wspomniany w poprzednim rozdziale **Google Chrome** czy **Mozilla Firefox**. Nie zapewniają one żadnych bardziej zaawansowanych mechanizmów maskujących naszą obecność w sieci (tryb incognito czy prywatny sprawia tylko, że przeglądarka nie zapisuje naszej aktywności i nie gromadzi danych na nasz temat). Ruch, który generujemy podczas korzystania z takich przeglądarek, jest łatwy do śledzenia, a nasz dostawca internetu (czyli ISP, od Internet Service Provider) dokładnie wie, jakie strony i kiedy odwiedzamy.

Google Chrome



Mozilla Firefox



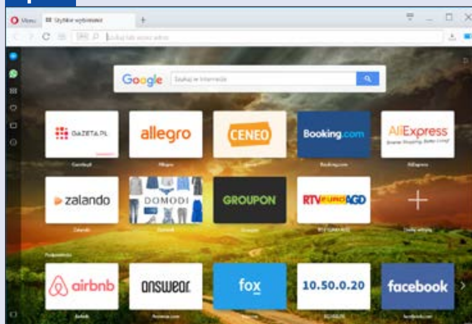
Bezpieczna przeglądarka

Przeglądarki bezpieczne to takie, które korzystają ze specjalnych mechanizmów anonimizujących, jak na przykład trasowanie cebulowe, VPN i inne, których głównym zadaniem jest ukrycie naszej obecności w sieci. Dobrym przykładem takiej przeglądarki jest **Tor Browser**. Na kolejnych stronach dowiemy się, jak działa, jak chroni naszą prywatność i jak z niego korzystać. Warto też zwrócić uwagę na przeglądarkę **Opera**, która pozwala za darmo korzystać z możliwości sieci VPN (w tym przypadku raczej serwera proxy), szczegóły działania tego mechanizmu również poznamy w tym rozdziale.

Tor Browser



Opera



filtrowania sieci i różnego typu ograniczeń w komunikacji i blokad regionalnych.

Trasowanie cebulowe

Działanie sieci Tor jest oparte na zasadzie **trasowania cebulowego**. Nazwa tego mechanizmu bierze się stąd, że z wykorzystaniem kryptografii, wielowarstwowo (stąd porównanie do cebuli) szyfrowane są wszystkie komunikaty przesyłane przez ciąg serwerów – ruterów cebulowych, które nie wiedzą, jakie dane przesyłają. Każdy może wspomóc taką sieć, uruchamiając na swoim komputerze serwer, który będzie jej służył. Prosta implementacja, jasne zasady działania i możliwość praktycznie całkowitego zniknięcia w internecie – to główne powody, dla których Tor odniósł duży sukces.

Czy można nas wyśledzić?

W teorii możliwe jest wyśledzenie użytkownika sieci Tor i potwierdzenie komunikacji wychodzącej i przychodzącej do jego komputera. Wymaga to jednak ogromnych środków i zaplecza technologicznego, by kontrolować jednocześnie węzeł początkowy i końcowy, kluczowe dla całej komunikacji. Według doniesień zdarza się to w Stanach Zjednoczonych. W naszym regionie takie potwierdzenie wystąpienia komunikacji jest praktycznie nie do przeprowadzenia.

Jak to działa w praktyce

Poznajmy podstawową zasadę działania Tora.

■ Normalne połączenie bez sieci Tor

Gdy normalnie korzystamy z internetu i chcemy odwiedzić jakąś witrynę, wpisujemy jej adres w przeglądarce. Jest on rozpoznawany i zostaje wysłane żądanie dostępu do adresu IP serwera tej witryny. Informacja o tym żądaniu jest przesyłana także do naszego dostawcy internetu wraz z logiem czasowym (kiedy żądanie wyszło z jakiego adresu IP i do jakiego IP docelowego ma dotrzeć). Tak więc przesyłane przez nas pakiety danych, nawet takie, które zawierają hasła i inne wrażliwe dane, są przechowywane na serwerach naszych dostawców internetu (jeśli korzystamy z witryn z protokołem HTTPS, dostawca wie tylko, o której godzinie jaką witrynę odwiedziliśmy, i nie ma dostępu do wrażliwych danych).

■ Połączenie z wykorzystaniem sieci Tor

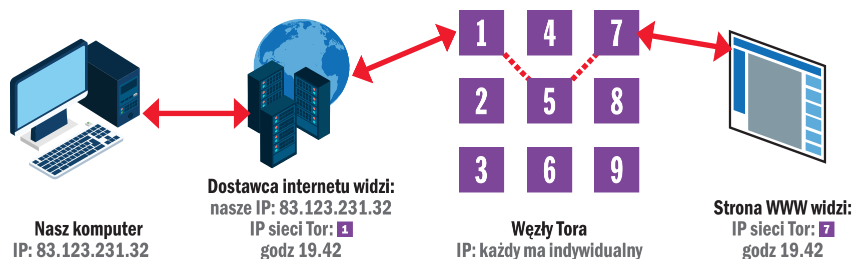
Gdy korzystamy z sieci Tor, całe żądanie dostępu do danej witryny jest szyfrowane i przesyłane do węzła początkowego. Nasz dostawca internetu wie tylko, o której godzinie z naszego adresu został wygenerowany pakiet wychodzący, jednak nie może sprawdzić treści takiego pakietu i widzi, że jego ruch kończy się na pierwszym węźle.
Tymczasem trasa pakietu jest znacznie dłuższa i przebiega przez wcześniej ustalony pseudo-

NORMALNE POŁĄCZENIE BEZ SIECI TOR



Bez Tora, gdy łączymy się z witryną w internecie, dane dotyczące naszego IP i całego połączenia trafiają bezpośrednio do dostawcy internetu oraz do serwera danej witryny

POŁĄCZENIE Z WYKORZYSTANIEM SIECI TOR



Gdy korzystamy z Tora, wybierana jest losowa trasa przez różne węzły sieci Tor. Dopiero ostatni węzeł odszyfrowuje nasz pakiet i wysyła go do właściwego serwera. Serwer nie wie, jaki jest nasz adres IP, a dostawca nie wie, z jakim serwerem się łączymy ani jakie dane przesyłamy

losowy (liczby pseudolosowe mają ukryte regularności nieistotne z punktu widzenia technicznego) szereg różnego typu węzłów, co pozwala na zwiększenie bezpieczeństwa i utrudnienie śledzenia. Dopiero ostatni węzeł, czyli węzeł końcowy, otrzymuje informację pozwalającą na odszyfrowanie pakietu i przesłanie go w normalny sposób do początkowego serwera. Serwer może odczytać pakiet i zna tylko czas dostępu i adres IP ostatniego węzła, a nie nasz. Właśnie dzięki temu jesteśmy anonimowi, gdyż nawet dostawca internetu nie jest w stanie stwierdzić, na jakie strony wchodzimy i jakie dane przesyłamy czy pobieramy z sieci. Jedyne, co rejestruje, to czas dostępu i ilość transmitowanych danych niezbędna do rozliczenia klienta.

Etykieta korzystania z sieci Tor

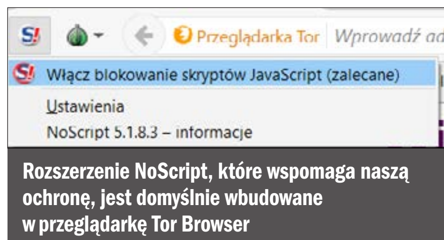
Ważne jest stosowanie się do podstawowych zasad, które mają na celu zachowanie optymalnej wydajności ruterów cebulowych dostarczanych przez ochotników i utrzymywanych na ich własny koszt. Stosowanie etykiety jest dobrowolne, ale ważne i w dobrym stylu – to internetowy savoir-vivre. Oto czego dotyczą jego cztery najważniejsze zasady.

- **Zbyt duży transfer danych** – źle postrzegane jest przesyłanie bardzo dużej ilości danych przy wykorzystaniu sieci Tor, ponieważ w znacznym stopniu może wpłynąć to na obciążenie całej sieci i spowolnienie pracy innych użytkowników.
- **Klienci torrent** – protokoły torrent nie powinny być wykorzystywane w sieci Tor, bo przeważnie służą pobieraniu nielegalnych treści i dużej ilości danych, co generuje zbyt duży ruch w sieci. Domyślnie polityka węzłów wyjściowych blokuje standardowe porty klientów torrent.
- **Spam** – jego rozsyłanie jest domyślnie zablokowane na węzłach wyjściowych na porcie 25, rozsyłanie spamu z sieci Tor jest wysoce niestosowne.
- **Specjalne traktowanie** – serwisy i witryny mają prawo inaczej traktować użytkowników rozpoznawanych jako korzystający z Tora. Przeważnie oznacza to zmniejszenie przepustowości lub inne ograniczenia.

UWAGA!
Wykorzystanie sieci anonimowej do dostępu do naszych kont używanych wcześniej w normalny sposób jest niebezpieczne i naraża naszą anonimowość. Łatwo odgadnąć, że to właśnie my używamy naszego konta, a identyfikację umożliwią czasy dostępu do serwerów.

Konfiguracja Tor Browser w Windows

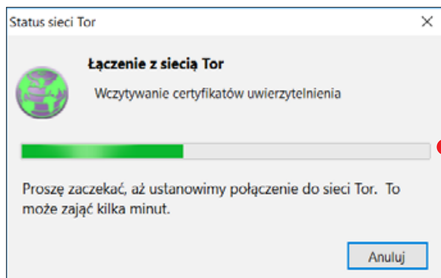
Tor Browser możemy zainstalować z płyty dołączonej do książki. Instalacja przebiega tak jak instalacja innych programów w Windows. Przeglądarka jest w języku polskim i dodatkowo ma wbudowane rozszerzenia, które wspomagają ochronę bezpieczeństwa i anonimowości, na przykład **NoScript**.



Rozszerzenie NoScript, które wspomaga naszą ochronę, jest domyślnie wbudowane w przeglądarkę Tor Browser

1 Przy pierwszym uruchomieniu przeglądarki pojawi się okno konfiguracyjne. W zdecydowanej większości przypadków wystarczy kliknąć na **Połącz**, aby przeglądarka rozpoczęła procedurę łączenia z siecią Tor. Jeśli jednak nasze łącze jest cenzurowane lub korzystamy z serwera proxy, wtedy musimy kliknąć na **Konfiguruj**.

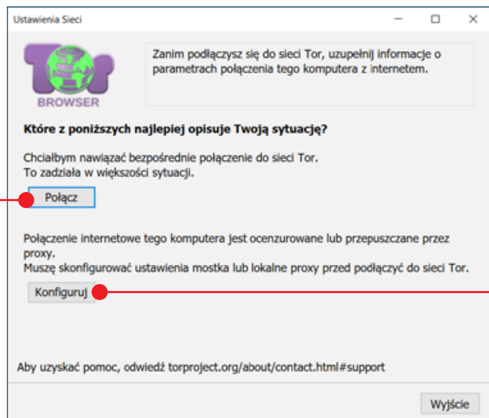
2 Pojawi się okno łączenia z siecią Tor. Na tym etapie pobierana jest lista wszystkich dostępnych węzłów, na podstawie których

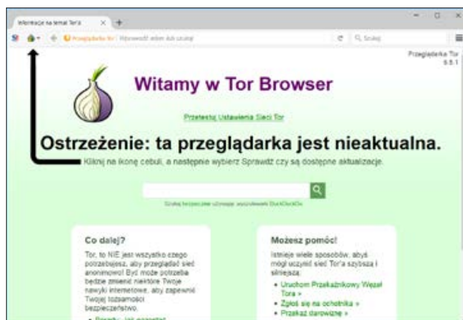


będzie tworzone połączenie, dzięki czemu staniemy się anonimowi w internecie. Dodatkowo wczytywane są specjalne certyfikaty uwierzytelnienia i inne informacje niezbędne do poprawnej pracy sieci. Ten proces powinien zakończyć się bez problemów, jeśli jednak się pojawią, może to oznaczać na przykład blokadę ze strony programu antywirusowego lub przez ustawienia firewalla.

Aktualizacje

Jeśli po uruchomieniu przeglądarki pojawi się informacja o tym, że jest ona nieaktualna, zanim zaczniemy korzystać z programu, koniecznie musimy jak najszybciej przeprowadzić jej aktualizację. Aktualizacje eliminują błędy i luki w zabezpieczeniach, a w sytuacji, gdy od funkcjonalności przeglądarki zależy

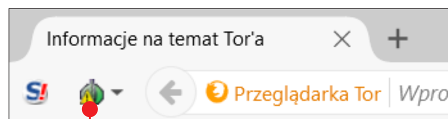




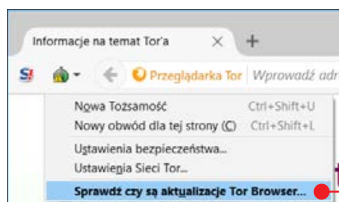
Domyślnie przeglądarka przy starcie sama sprawdza, czy jest dostępna nowa wersja oprogramowania, i informuje nas o tym na stronie głównej

nasza anonimowość, nie możemy sobie pozwolić na narażanie się na niebezpieczeństwo przez odkładanie aktualizacji.

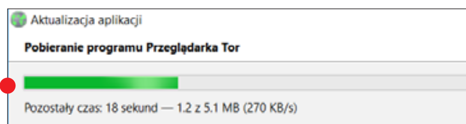
1 W celu zaktualizowania przeglądarki klikamy na pasku nawigacyjnym na ikonę cebuli. Dodatkowo o niebezpieczeństwie informuje nas trójkąt ostrzegawczy.



2 Następnie klikamy na **Sprawdź, czy są aktualizacje Tor Browser...**.



3 Uruchomiony zostanie aplet wyszukujący i pobierający aktualizacje. Cały proces przebiega automatycznie – nie musimy nic robić. Po jego zakończeniu i ponownym uruchomieniu przeglądarki możemy korzystać z nowej, aktualnej wersji.



Wybieramy poziom bezpieczeństwa

Zanim zaczniemy korzystać z przeglądarki na dobre, ważne jest wybranie odpowiedniego dla nas poziomu bezpieczeństwa. Ustalamy, na jakim poziomie zabezpieczeń i anonimowości nam zależy. To ustawienie możemy później zmienić, jeśli przestanie nam odpowiadać.

TRZY POZIOMY BEZPIECZEŃSTWA DO WYBORU

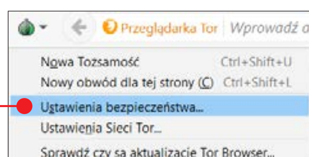
1 **Niski** (domyślny) – jest to standardowy poziom przeznaczony dla użytkowników, którzy nie potrzebują mocnej ochrony i nie zależy im na zachowaniu maksymalnej anonimowości.

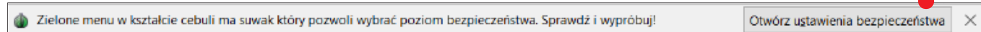
2 **Średni** – ten poziom oferuje najbardziej optymalne ustawienia ochrony, które nie wpływają w znaczący sposób na komfort korzystania z przeglądarki. Między innymi nie pozwala na uruchamianie skryptów na stronach bez protokołu HTTPS i nie pozwala na automatyczne wyświetlanie elementów audio i wideo bez zgody użytkownika. Zaleca się wypróbowanie tego właśnie poziomu od razu po zainstalowaniu przeglądarki.

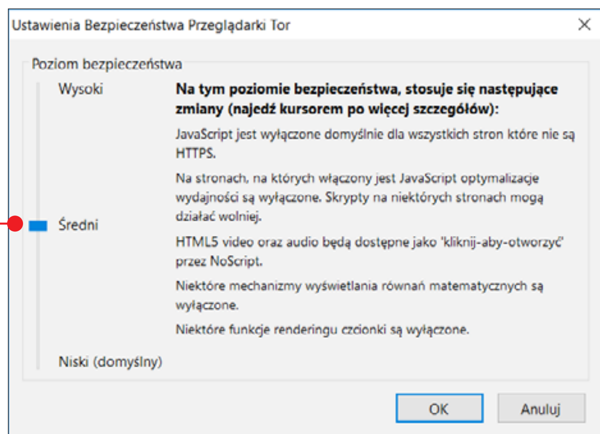
3 **Wysoki** – oferuje ochronę na najwyższym poziomie. Skrypty wyłączone są na wszystkich typach stron, a dodatkowo mogą być blokowane na przykład pliki czcionek i obrazów. Dotyczy to też filmów i plików audio. Sprawia to, że korzystanie z przeglądarki w tym trybie jest niekomfortowe i czasem nawet uciążliwe dla zwykłego użytkownika.

1 Przy pierwszym uruchomieniu przeglądarki pod górnym paskiem pojawi się informacja o ustawieniu poziomu bezpieczeństwa – aby przejść dalej, wystarczy kliknąć na **Otwórz ustawienia bezpieczeństwa**.

2 Możemy również w każdej chwili przejść do tych ustawień, klikając na ikonę cebuli, a następnie na **Ustawienia bezpieczeństwa**.







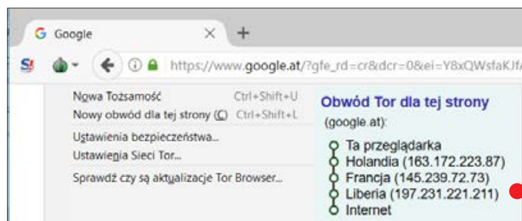
3 Do wyboru mamy trzy ustawienia. Wystarczy wybrać poziom ochrony, który jest nam potrzebny, i kliknąć na **OK**.

4 Teraz możemy rozpocząć korzystanie z przeglądarki.

Obwód Tor a adres IP

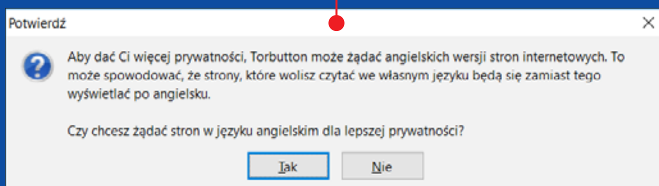
Po wejściu na jakąkolwiek stronę internetową będziemy mogli sprawdzić nasz obwód Tor, czyli drogę poprzez poszczególne węzły sieci Tor od wejściowego do wyjściowego. W naszym przykładzie ruch kierowany jest przez trzy różne kraje i przez trzy różne adresy IP. Naszym finalnym adresem jest adres węzła znajdującego się na samym dole, w tym przypadku **Liberia**. Nasz adres początkowy nie ma tutaj znaczenia, gdyż każda strona, z którą będziemy się łączyli, będzie w stanie rozpoznać tylko i wyłącznie adres IP ostatniego węzła sieci Tor. Jest to szczególnie istotne w wypadku blokad regionalnych, gdy jakieś treści w internecie nie są dostępne na przykład dla użytkowników z Polski lub Europy, a tylko w USA. Jeśli adres IP końcowego węzła będzie właśnie z USA, zostaniemy dopuszczeni do treści za blokadą.

W każdej chwili możemy „zmienić tożsamość”, czyli wylosować nowe węzły dla całej przeglądarki lub nowy obwód tylko dla wybranej strony. Oto jak to zrobić.



ANONIMOWOŚĆ NA JESZCZE WYŻSZYM POZIOMIE

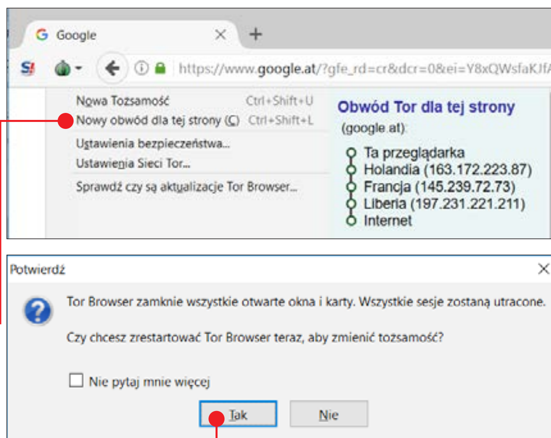
Jeśli zależy nam na jak największej anonimowości, możemy zdecydować się na ustawienie żądania angielskich wersji stron internetowych. Dzięki temu jeszcze bardziej ukryjemy się w internecie. Dlaczego? Otóż kiedy węzeł końcowy ze Szwecji żąda wyświetlenia witryny google.com w języku polskim, jest to bardziej podejrzane, niż gdy żądanie końcowe jest w języku angielskim. Tę funkcję możemy w każdej chwili aktywować w opcjach przeglądarki (możemy też wyrazić zgodę na jej aktywację przy pierwszym wpisaniu adresu internetowego).



1 Gdy nasz końcowy węzeł jest w nieodpowiednim kraju, w którym na przykład również nie ma dostępu do blokowanej treści, klikamy na ikonę cebuli na górnym pasku nawigacyjnym przeglądarki.

2 Następnie wybieramy opcję **Nowa Tożsamość** lub **Nowy obwód dla tej strony** ●.

3 Przeglądarka zostanie ponownie uruchomiona – zatwierdzamy restart programu, klikając na **Tak** ●.



WARTO PAMIĘTAĆ

Mimo że Tor zapewnia anonimowość i wysoki poziom ochrony, musimy pamiętać, że jeśli, korzystając z niego, będziemy wstawiać wpisy ze swoich kont społecznościowych lub logować się na witryny bez szyfrowania SSL, sami narazimy swoją anonimowość. Przeglądarki Tor powinniśmy używać w szczególnych przypadkach, gdy zachowanie anonimowości jest potrzebne, a nie wtedy, gdy będziemy chcieli na przykład obejrzeć film na YouTube.

4 Po ponownym uruchomieniu programu zobaczymy, że nasz obwód został zmieniony – końcowy węzeł będzie już w innym kraju ●.



Co to jest VPN?

VPN to **Wirtualna Sieć Prywatna** (ang. Virtual Private Network). Popularnie połączenia w takiej sieci nazywa się **tunelowanymi**, ponieważ transmisja pakietów jest zaszyfrowana pomiędzy dwoma punktami, które w ten sposób tworzą „tunel" w internecie. Takie rozwiązania sieciowe są wykorzystywane w firmach, ponieważ zapewniają wysoki poziom bezpieczeństwa przy niskich kosztach. Pracownik może uzyskać zdalny dostęp do zasobów w firmie w każdej chwili, a przy tym nikt postronny nie będzie mógł się dowiedzieć, jakie dane są przesyłane.

Dla domowego użytkownika wykorzystanie sieci VPN jest również bardzo atrakcyjne, ponieważ pozwala w bezpieczny i anonimowy sposób uzyskać dostęp do zasobów internetu. Jest to niezwykle przydatne na przykład wtedy, gdy jesteśmy zmuszeni do korzystania z otwartych sieci lub publicznych hotspotów.

Przy normalnym połączeniu administrator sieci i dostawca internetu mają wgląd w nasze pakiety, jednak jeśli skorzystamy z możliwości połączeń z siecią VPN, ruch, który będziemy generować, zostanie zaszyfrowa-

ny i będziemy mogli na przykład bez obaw, w bezpieczny sposób skorzystać z bankowości internetowej.

Typy sieci VPN

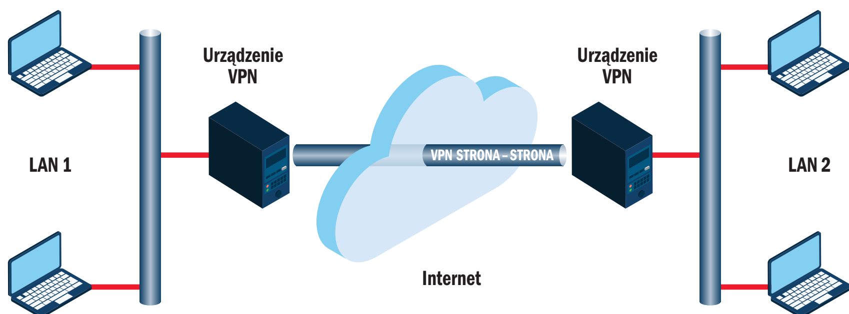
Rozróżniamy dwa podstawowe typy sieci VPN.

- **Strona – Strona** – jest to przykład rozszerzenia sieci firmowej; pozwala na uzyskanie dostępu pomiędzy dwoma odległymi sieciami LAN, które łączą się ze sobą poprzez sieć publiczną. Są wykorzystywane między innymi przez program **OpenVPN**.
- **Klient – Strona** – to bardziej zaawansowane rozwiązanie, które przeznaczone jest do pracy ze zdalnymi serwerami.

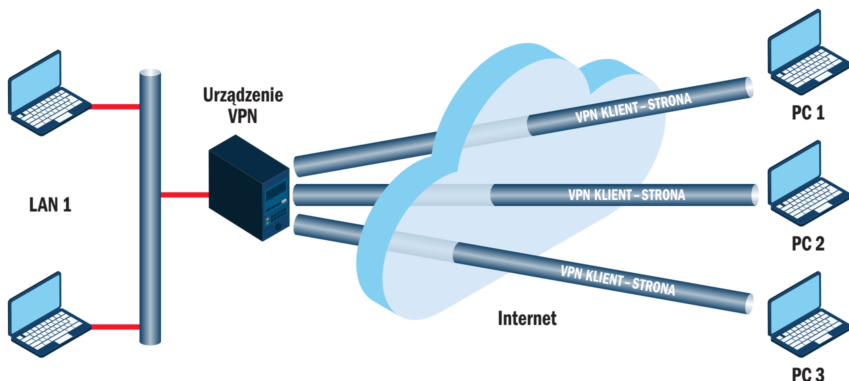
Protokoły i szyfrowanie

Protokoły sieci VPN to inaczej protokoły komunikacyjne z określonymi regułami i zasadami, które mają pozwolić na bezpieczne nawiązania łączności między dwoma punktami. Oto kilka popularnych protokołów sieci VPN.

TYPY SIECI VPN: STRONA – STRONA



TYPY SIECI VPN: KLIENT – STRONA



PPTP

Jeśli korzystamy z tego typu protokołu, to powinniśmy jak najszybciej przestać. Ma on kilka zalet, ale brak bezpieczeństwa całkowicie przekreśla jego przydatność, także Microsoft odradza jego używanie. Niestety, nadal jest używany przez wiele firm i użytkowników nieświadomych potencjalnego zagrożenia.

Zalety:
- szybkie działanie, prostota nie wpływa na wydajność
- łatwa konfiguracja
- dostępny na praktycznie każdym urządzeniu

Wady:
- nawet silnie zabezpieczona sesja może być złamana w ciągu 24 godzin
- brak mocnego szyfrowania

L2TP/IPSec

Jest to hybryda dwóch protokołów, samo L2TP pozwala tylko na utworzenie tunelu komunikacyjnego i przesyłanie danych. Za bezpieczeństwo odpowiedzialny jest protokół IPSec, który odpowiada za uwierzytelnianie i szyfrowanie połączenia. Zapewniał wysokie bezpieczeństwo, jednak po ujawnieniu przez Edwarda Snowdena informacji o NSA można przyjąć, że protokół IPSec nie daje wcale tak wysokiej ochrony i może być złamany przez służby specjalne.

Zalety:
- szybkość działania
- wysokie bezpieczeństwo
- powszechnie dostępny w różnych systemach

Wady:
- istnieje wysokie ryzyko złamania protokołu IPSec przez NSA, co może stanowić zagrożenie
- działa na porcie UDP 500, przez co łatwo wykryć korzystanie z sieci VPN; niektórzy usługodawcy internetu oraz hotspoty mogą blokować ten port

OpenVPN

Kolejna hybryda różnych protokołów, która zapewnia najwyższy stopień ochrony; nie ma żadnych informacji, które sugerowałyby złamanie jego zabezpieczeń. Wykorzystuje bibliotekę OpenSSL i protokoły SSLv3 oraz TLSv1. Pozwala to na korzystanie z najlepszych form szyfrowania połączenia i zabezpieczania sesji. Dodatkowo możemy łączyć się za pomocą dowolnego portu, dzięki czemu unikniemy wykrycia, że korzystamy z połączenia z siecią VPN.

Zalety:
- otwarty kod źródłowy
- najwyższy poziom bezpieczeństwa
- szerokie możliwości konfiguracji

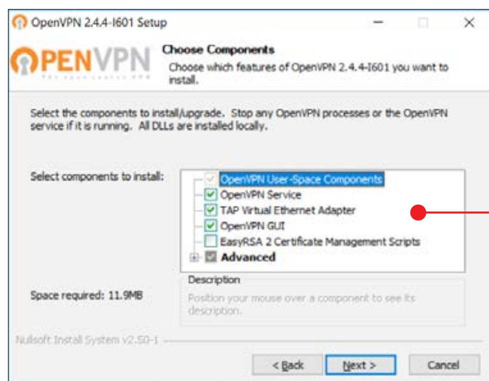
Wady:
- wymaga instalacji specjalnej aplikacji
- konfiguracja może sprawić trudności początkującym użytkownikom

Konfiguracja OpenVPN w Windows 10

Jeśli zależy nam na bezpieczeństwie i anonimowości, najlepszym wyborem jest skorzystanie z protokołu OpenVPN. Przeczytajmy, jak korzystać z niego w systemie Windows: od instalacji specjalnej aplikacji, poprzez jej konfigurację, po korzystanie z tunelowego połączenia.

Instalujemy klienta sieci OpenVPN

1 Instalacja przebiega typowo dla systemu Windows, ważne jednak, żeby pozostawić zaznaczone domyślne opcje instalacyjne, gdyż ich zmiana może uniemożliwić późniejsze korzystanie z programu w przedstawiony dalej sposób.



2 Musimy również wyrazić zgodę na instalację specjalnego sterownika wirtualnej sieci, bez którego nie będzie możliwe łączenie się z serwerami.

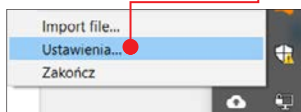
Konfigurujemy klienta OpenVPN

Po uruchomieniu programu nie będziemy mogli od razu skorzystać z możliwości bezpiecznego połączenia – musimy dograć pliki konfiguracyjne, które na to pozwolą.

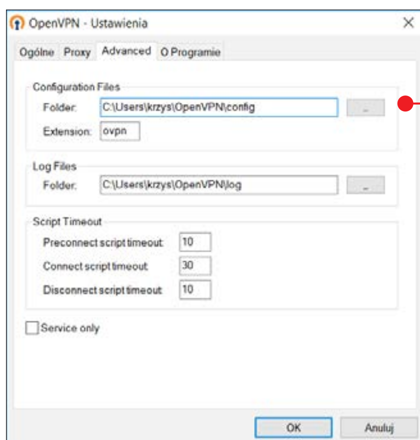
1 Uruchamiamy **OpenVPN GUI**.



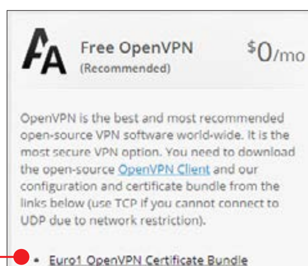
2 Następnie klikamy prawym przyciskiem myszy na ikonę w zasobniku systemowym, a później na **Ustawienia**.



3 Przechodzimy do zakładki **Advanced** i sprawdzamy lokalizację folderu, w którym powinny być pliki konfiguracyjne. Otwieramy Eksplorator i nawigujemy do tej lokalizacji.



4 Uruchamiamy przeglądarkę i wchodzimy na adres **https://www.vpnbook.com/freevpn** (możemy również skorzystać z innych stron oferujących darmowy lub płatny dostęp do serwerów VPN). Na podanej stronie klikamy na **Euro1 OpenVPN Certificate Bundle** i pobieramy plik z rozszerzeniem ZIP.



5 Wypakowujemy zawartość archiwum do folderu przeznaczonego na pliki konfiguracyjne ●.

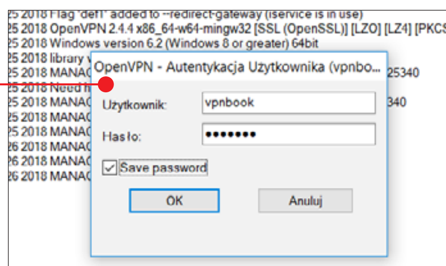
Ten komputer > Dysk lokalny (C:) > Użytkownicy > krzys > OpenVPN > config

Nazwa	Data modyfikacji	Typ	Rozmiar
vpnbook-euro1-tcp80	26.11.2014 08:36	OpenVPN Config F...	4 KB
vpnbook-euro1-tcp443	26.11.2014 08:36	OpenVPN Config F...	4 KB
vpnbook-euro1-udp53	26.11.2014 08:36	OpenVPN Config F...	4 KB
vpnbook-euro1-udp25000	26.11.2014 08:36	OpenVPN Config F...	4 KB

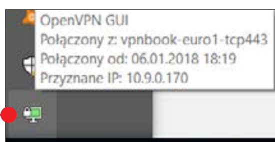
6 Teraz zamykamy i ponownie uruchamiamy klienta OpenVPN. Po kliknięciu na ikonę klienta zobaczymy cztery serwery, z którymi możemy nawiązać połączenie. Wystarczy najechać kursorem na dany serwer, a następnie kliknąć na **Połącz** ●.

vpnbook-euro1-tcp443 > | Połącz
vpnbook-euro1-tcp80 > | Rozłącz
vpnbook-euro1-udp25000 > | Pokaż Status
vpnbook-euro1-udp53 > | Pokaż Log

7 Pojawi się okno z prośbą o podanie loginu i hasła ●, dla przykładowego serwera są to odpowiednio **vpnbook** i **jmm66cf**. Zaznaczamy **Save password** i klikamy na **OK**.



8 Po poprawnym zestawieniu połączenia ikona klienta OpenVPN ● zmieni kolor na zielony.



9 Po sprawdzeniu naszego adresu IP i po zestawieniu połączenia okaże się, że łączymy się szyfrowanym połączeniem z serwerem w Rumunii ●.

Geolocation data from IP2Location (Product: DB6, updated on 2018-1-1)

IP Address	Country	Region	City
176.126.237.217	Romania	Bucuresti	Bucharest
ISP	**Organization**	**Latitude**	**Longitude**
AliStar Security SRL	Not Available	44.4323	26.1063

Uwaga! Strony internetowe będą się wczytywały wolniej, zwłaszcza podczas łączenia z darmowymi serwerami OpenVPN. Jest to jednak wystarczająca szybkość, by na przykład swobodnie korzystać z poczty lub innych serwisów, jak Facebook czy Twitter. Wolniejsze łącze to mały dyskomfort w porównaniu ze wzrostem naszego bezpieczeństwa w sieci. W ustawieniach możemy skonfigurować autostart programu wraz z Windows, dzięki czemu automatycznie będziemy korzystać z wybranego połączenia z serwerem VPN. Możemy w każdej chwili rozłączyć się z wybranym serwerem.

OPERA A VPN

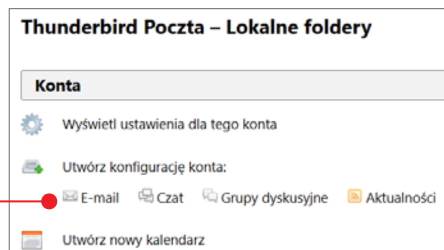
Przeglądarka Opera ma opcję, która jest reklamowana jako wbudowany w nią VPN z nieograniczonym transferem (znajdziemy ją w ustawieniach). Usłudze tej bliżej jednak do zwykłego połączenia typu proxy. Ruch przeglądarki przekierowywany jest szyfrowanym połączeniem na serwery firmy SurfEasy, która należy do producenta Opery. Cały ruch sieciowy naszego komputera nie jest w żaden sposób zabezpieczony. Jest to oczywiście nadal wygodna opcja i zapewnia lepszą ochronę niż zwykłe przeglądarki, jednak może dawać mylne poczucie bezpieczeństwa i anonimowości – nazwa funkcji nie do końca odpowiada rzeczywistości.

Bezpieczne wiadomości e-mail

W rozdziale drugim poznaliśmy już programy, które potrzebne będą do wygodnej i bezpiecznej komunikacji e-mail. Przeczytajmy teraz, jak w praktyce skonfigurować pocztę i zacząć korzystać z bezpiecznych wiadomości na co dzień.

Klient poczty e-mail

Jeśli zależy nam na anonimowości na najwyższym poziomie, powinniśmy założyć bezpieczne konto e-mail w takim serwisie, jak na przykład **Autistici**, **Kolab Now** czy **Riseup** i korzystać tylko z niego. Możemy także używać kont oferowanych przez duże firmy i stosować szyfrowanie, jednak wtedy istnieje ryzyko, że nasze wiadomości są gdzieś przechowywane i w każdej chwili ktoś niepowołany może uzyskać do nich dostęp.

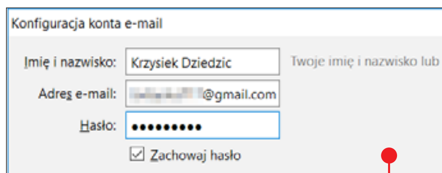


W tym poradniku poznamy program **Mozilla Thunderbird**, który jest bardzo wszechstronny i zarazem odpowiednio bezpieczny.

1 Instalujemy klienta poczty Thunderbird.

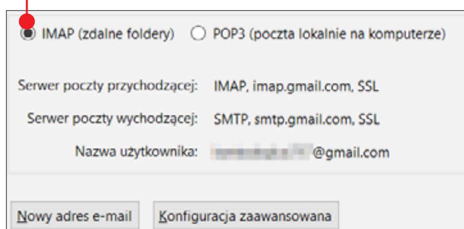
2 Uruchamiamy program i w głównym oknie interfejsu w polu **Konta** klikamy na **E-mail**.

3 Następnie klikamy na **Pomiń i użyj istniejącego adresu e-mail**.

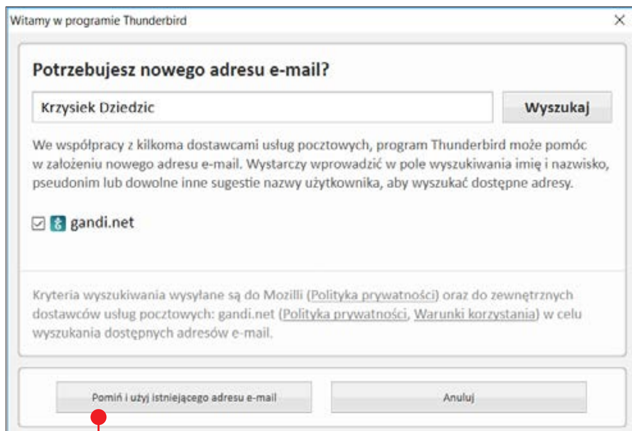


4 Teraz podajemy wymagane dane i klikamy na **Kontynuuj**.

5 Następnie program powinien prawidłowo rozpoznać serwery e-mail naszego konta. Upewniamy się, czy przy obydwu pozycjach na końcu jest **SSL** lub **STARTTLS**, co oznacza wsparcie szyfrowania. Pozostawiamy zaznaczoną opcję **IMAP** i klikamy na **Gotowe**.



6 Możemy już uzyskać dostęp do konta pocztowego przez Thunderbirda.

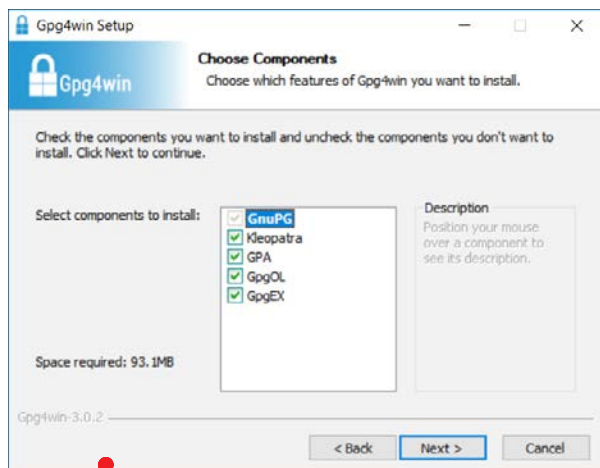


Klient GPG

Jest to specjalny program służący do generowania kluczy, które pozwolą nam szyfrować nasze wiadomości i je odszyfrowywać. Jest niezbędny do konfiguracji bezpiecznej poczty e-mail.
Potrzebne będą nam dwa klucze – prywatny i publiczny.

- **Klucz prywatny** – jest to najważniejszy klucz, który powinien być znany wyłącznie nam i tylko nam. Służy on do zaszyfrowywania, podpisywania i odszyfrowywania naszych wiadomości.
- **Klucz publiczny** – to specjalny klucz, którym będziemy dzielić się z osobami, z którymi zamierzamy wymieniać zaszyfrowane wiadomości. My musimy przesłać taki klucz naszym odbiorcom, a oni nam. Dopiero wtedy będzie możliwa zabezpieczona komunikacja.

Jeśli chcemy skonfigurować tego typu ustawienia, musimy zainstalować program **Gpg4win**, który służy do obsługi wyżej wymienionych kluczy (patrz rozdział drugi).



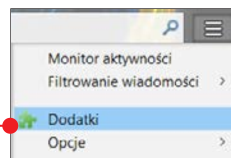
Instalujemy dodatek Enigmail dla Thunderbirda

Po zainstalowaniu Gpg4win (opis w rozdziale drugim) możemy zainstalować dodatek **Enigmail**, który pozwoli na korzystanie z szyfrowania w programie Thunderbird.

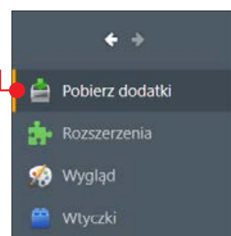
UWAGA!

Wszystkie e-maile są przechowywane na naszym dysku i nawet jeśli stosujemy szyfrowanie wysyłanych wiadomości, osoby trzecie mogą uzyskać do nich dostęp bezpośrednio z naszego dysku. Jeżeli zależy nam na bezpieczeństwie, powinniśmy zadbać o zaszyfrowanie dysku lub chociaż lokalizacji, gdzie są wrażliwe dane, czyli właśnie folderu z pocztą e-mail.

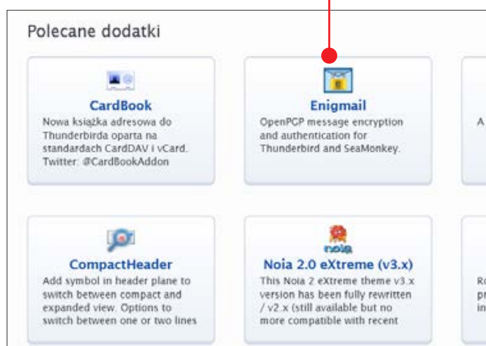
1 Po uruchomieniu Thunderbirda klikamy na trzy kreski w prawym górnym rogu, a następnie na **Dodatki**.



2 Następnie po lewej stronie klikamy na **Pobierz dodatki**.



3 Teraz wyszukujemy dodatek **Enigmail**, powinien być w oknie po prawej stronie w dziale **Polecane dodatki**. Jeśli go tam nie będzie, musimy kliknąć na **Zobacz wszystkie**, wpisać w wyszukiwarkę **Enigmail** i przejść do dodatku.





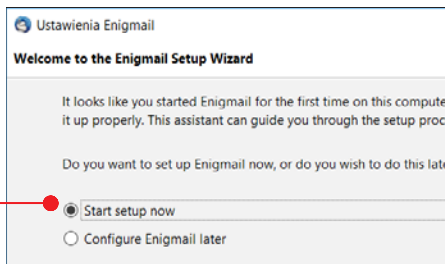
4 Następnie klikamy na **Zainstaluj** ● i potwierdzamy instalację dodatku z nieznanego źródła. Konieczne jest ponowne uruchomienie programu Thunderbird.

Konfiguracja dodatku Enigmail

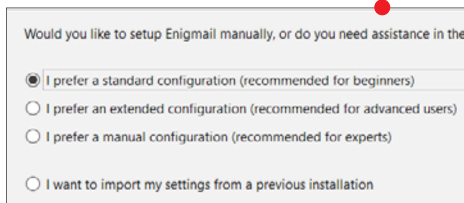
Cały proces nie jest zbyt skomplikowany, chociaż dodatek jest dostępny w języku angielskim. Należy stosować się do poniższych porad, a wszystko przebiegnie szybko i bezproblemowo.

1 Po ponownym uruchomieniu programu Thunderbird uruchomi się automatycznie konfiguracja dodatku Enigmail.

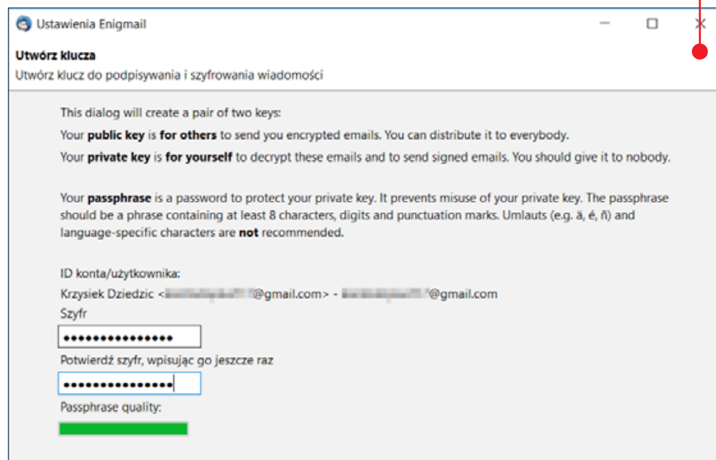
2 Pozostawiamy zaznaczoną domyślną opcję **Start setup now** ● i klikamy na **Dalej**.



3 W kolejnym oknie ● również nic nie zmieniamy i klikamy na **Dalej**.

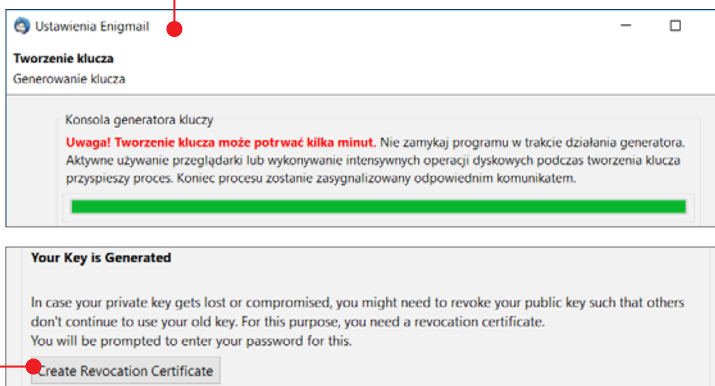


4 Teraz przechodzimy do ważnej części konfiguracji – tworzymy hasło ●, które będzie chroniło nasz klucz prywatny. Jest on niezwykle ważny – dlatego postarajmy się, aby hasło było silne. **Uwaga!** Nie stosujemy znaków diaktrycznych w haśle. Klucz publiczny i prywatny zostaną wygenerowane automatycznie i o ich bezpieczeństwo nie musimy się martwić. Po podaniu hasła klikamy na **Dalej**.

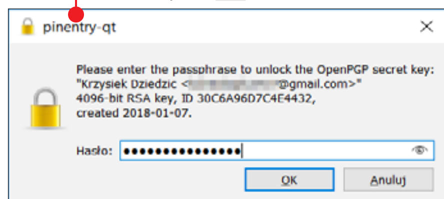


5 Rozpocznie się generowanie pary kluczy indywidualnych specjalnie dla nas. Może potrwać dość długo ●. Przyspieszymy ten proces, jeśli w jego trakcie będziemy aktywnie korzystać z klawiatury lub z przeglądarki. Proces polega na zbieraniu losowych danych i trwa długo, bo klucze publiczny i prywatny są naprawdę złożone i rozbudowane.

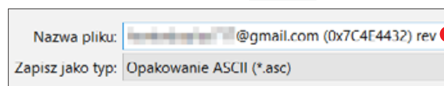
6 Teraz powinniśmy wygenerować **Revocation Certificate**, który służy do unieważniania naszych kluczy, co może być przydatne wtedy, gdy stracimy dostęp do klucza prywatnego, będziemy chcieli używać nowej pary kluczy itp. Klikamy na **Create Revocation Certificate**.



7 Pojawi się specjalne okno, w którym musimy podać nasze wcześniej utworzone hasło. Klikamy na **OK**.



8 Teraz wybieramy lokalizację, w której zapiszemy nasz certyfikat do unieważniania kluczy, i klikamy na **Zapisz**.

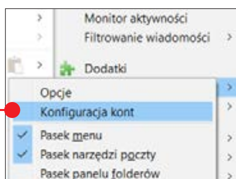


9 Możemy wrócić do konfiguratora, przejść dalej i zakończyć jego pracę.

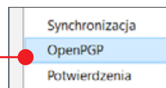
Dodajemy funkcje szyfrowania wiadomości w Thunderbirdzie

Po skonfigurowaniu dodatku możemy dodać jego funkcje do naszego konta e-mail w aplikacji Thunderbird.

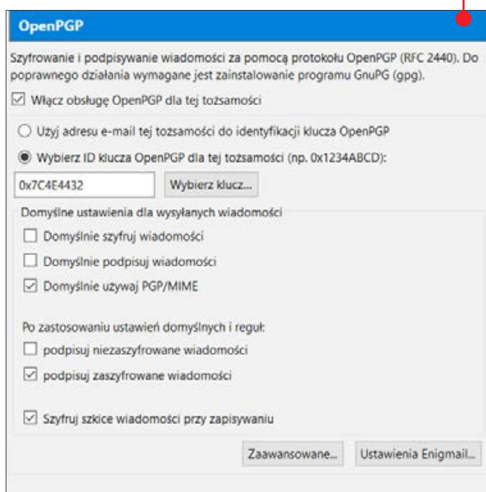
1 Uruchamiamy program Thunderbird, klikamy na trzy kreski w prawym górnym rogu i na **Opcje**, **Konfiguracja kont**.



2 Po lewej stronie klikamy na **OpenPGP** w celu przejścia do ustawień szyfrowanych wiadomości.



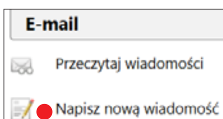
3 Po prawej stronie będą widoczne ustawienia. Jeśli wszystko zostało przez nas poprawnie skonfigurowane w poprzedniej wskazówce, nasze konto e-mail powinno zostać automatycznie wykryte razem z numerem identyfikacyjnym. Zaznaczamy opcję **Domyślnie używaj PGP/MIME** (lepsze szyfrowanie załączników) i **Podpisuj zaszyfrowane wiadomości** (cyfrowe podpisywane zaszyfrowane wiadomości z tego konta) i klikamy na **OK**.



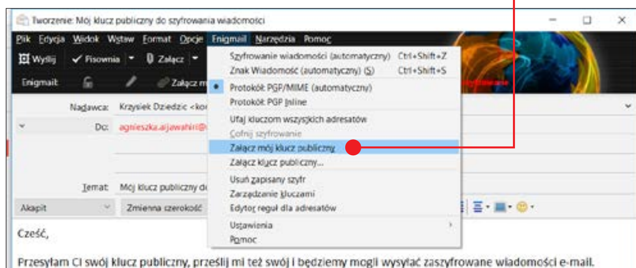
Wysyłamy nasz klucz publiczny

Jeśli chcemy wysyłać zaszyfrowane wiadomości, musimy przesłać naszym odbiorcom nasz klucz publiczny, a oni muszą przesłać nam swoje klucze publiczne. Możemy tego dokonać przy użyciu zwykłego e-maila z załącznikiem.

1 Po uruchomieniu programu Thunderbird klikamy na **Napisz nową wiadomość**.



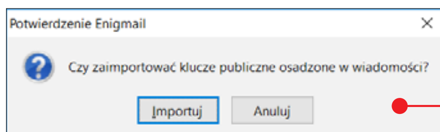
2 Wpisujemy treść e-maila i adres odbiorcy, a następnie na górnym pasku klikamy na **Enigmail**, **Załącz mój klucz publiczny**. Teraz wystarczy kliknąć na **Wyślij** w lewym górnym rogu i poczekać, aż nasz odbiorca prześle nam swój klucz.



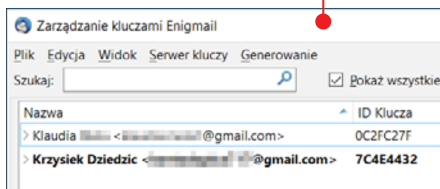
Importujemy i zatwierdzamy klucze publiczne

1 Po odebraniu wiadomości e-mail, która zawiera klucz publiczny, wystarczy kliknąć na niego prawym przyciskiem myszy, a następnie wybrać opcję **Importuj klucz OpenPGP**. Jeśli klucz zostanie automatycznie wykryty, wystarczy kliknąć na **Import Key**.

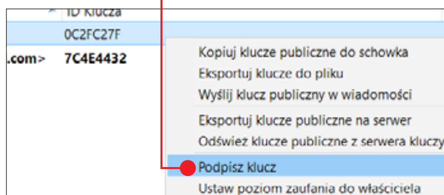
2 Następnie wyrażamy zgodę na import i po chwili powinno pojawić się okno z informacją o sukcesie.

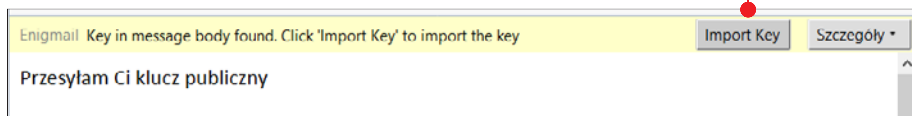


3 Teraz na górnym pasku Thunderbirda najeżdżamy na **Enigmail** i klikamy na **Zarządzanie kluczami**. W oknie zobaczymy nowo dodany klucz publiczny, zanim jednak rozpoczniemy przesyłanie zaszyfrowanych wiadomości, nasz odbiorca i my musimy potwierdzić i podpisać wybrany klucz, żeby Enigmail wiedział, że na pewno jest on prawidłowy.

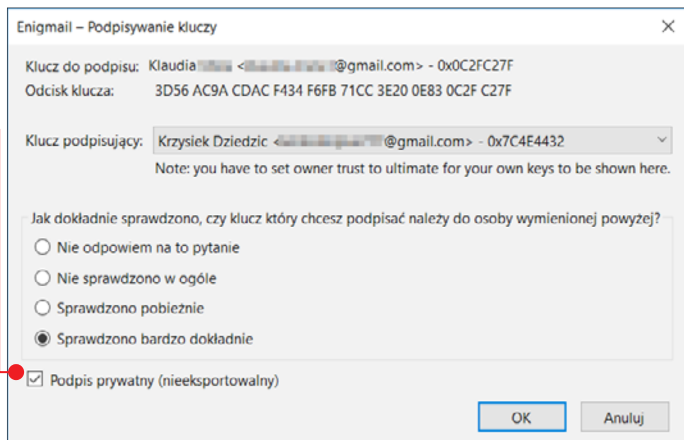


4 Potwierdzenie klucza najlepiej przeprowadzić przez telefon lub w bezpośredniej rozmowie. Polega ono na upewnieniu się, że wszystkie znaki w kluczu są poprawne. Możemy później przystąpić do podpisania takiego klucza – wystarczy kliknąć na niego prawym przyciskiem myszy i z menu wybrać opcję **Podpisz klucz**.





5 W nowym oknie wybieramy **Sprawdzono bardzo dokładnie** i zaznaczamy **Podpis prywatny (nieeksportowalny)**. Klikamy na **OK**.



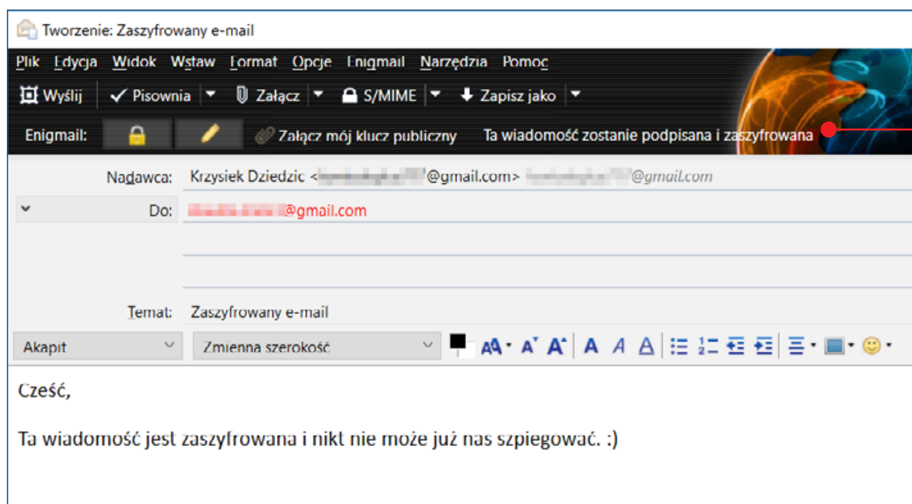
6 Podajemy nasze hasło klucza prywatnego i klikamy na **OK** w celu podpisania klucza publicznego osoby, z którą będziemy korespondować.

7 To koniec całego procesu konfiguracyjnego.



Wysyłamy i odbieramy zaszyfrowane wiadomości

Teraz przy korzystaniu z programu Thunderbird za każdym razem, gdy będziemy wysyłać wiadomość do kontaktu, który udostępnił nam swój klucz publiczny, a którym podpisaliśmy, wiadomości będą automatycznie szyfrowane. Będą również automatycznie rozszyfrowywane, gdy nasz odbiorca nam odpisze. Na górnym pasku będziemy widzieli ikonę kłódki i długopisu oraz informację **Ta wiadomość zostanie podpisana i zaszyfrowana** – wtedy będziemy mieli pewność, że nikt nie podejrzy naszych e-maili i że możemy całkowicie anonimowo korzystać z poczty.



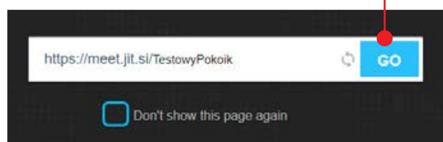
Jitsi: anonimowa alternatywa dla Skype'a

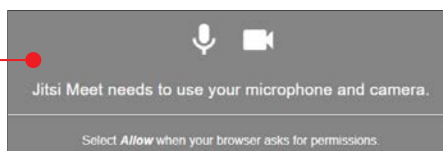
Jeśli zależy nam na anonimowości w każdej usłudze, możemy zamiast Skype'a użyć ogólnie dostępnego programu **Jitsi**. Nie jest wymagane instalowanie klienta Jitsi na naszym komputerze, jeśli zamierzamy tylko sporadycznie komunikować się z kimś na wideoczacie przy tak wysokim poziomie bezpieczeństwa. Możemy skorzystać z możliwości oferowanych online w przeglądarce.



Fot. Wavebreakmedia Ltd/Dreamstime.comcom

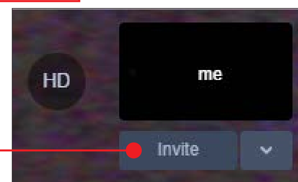
1 Wchodzimy na stronę **https://meet.jit.si/**, a następnie dopisujemy nazwę pokoju rozmów, który chcemy utworzyć, i klikamy na **GO**.





2 Teraz musimy wyrazić zgodę na wykorzystywanie przez przeglądarkę naszego mikrofonu i kamery.

3 Następnie w prawym górnym rogu klikamy na **Invite**.



4 Potem klikamy na **Add password**, w celu zabezpieczenia naszej rozmowy hasłem.

5 Wpisujemy złożone hasło i klikamy na **Add**. Pojawi się informacja o tym, że rozmowa została zabezpieczona.

6 Teraz wystarczy przesłać na przykład zaszyfrowaną wiadomością link i hasło do utworzonej rozmowy. Możemy również wcześniej umówić się z kimś na nazwę pokoju i hasło, dzięki czemu nie będziemy musieli nawet przesyłać tej informacji.
Jest to w pełni bezpieczna i anonimowa platforma, która ma bardzo duże możliwości. Dzięki niej możemy w anonimowy sposób rozmawiać ze znajomymi i nikt nie podsłucha ani nie przechwyci naszych rozmów. Jeśli chcemy, możemy zainstalować program Jitsi i korzystać z niego jak z komunikatora.



MOBILNE ROZWIĄZANIA: SIGNAL – ANONIMOWE WIADOMOŚCI NIE DO NAMIERZENIA

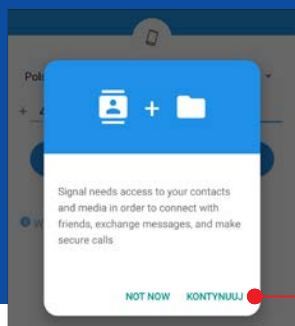
Jest to jedna z najbezpieczniejszych aplikacji do szyfrowanej komunikacji. Dostępna jest na popularne systemy mobilne, jak również w wersji na systemy stacjonarne. Cała komunikacja jest szyfrowana i nikt oprócz naszych odbiorców nie będzie w stanie jej rozszyfrować. Nawet twórcy aplikacji nie są w stanie stwierdzić, o czym rozmawiamy i jakiego typu wiadomości przesyłamy. Oprócz przesyłania wiadomości tekstowych, zdjęć, plików możemy również nawiązywać połączenia głosowe. Wszystkie te usługi realizowane są poprzez internet. Nie używają naszej karty SIM, więc żadne informacje nie zostaną zachowane także przez operatora sieci komórkowej. Jest to idealne rozwiązanie dla osób szukających prywatności i bezpieczeństwa przy wymianie informacji na urządzeniach mobilnych.

Konfigurujemy Signal na smartfonie z Androidem

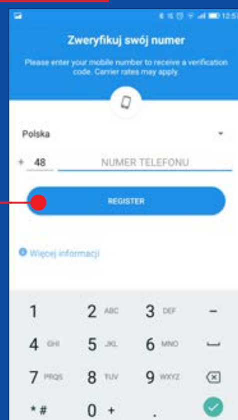
1 Pobieramy i instalujemy Signal ze Sklepu Play.

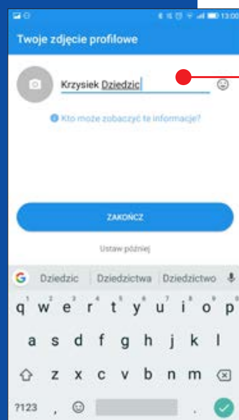


2 Następnie uruchamiamy aplikację na naszym urządzeniu. Od razu po uruchomieniu musimy przyznać jej prawa dostępu. Wystarczy nacisnąć **Kontynuuj**.



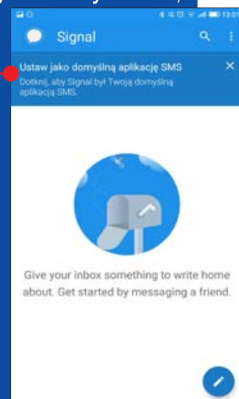
3 Następnie musimy podać nasz numer telefonu w celu zweryfikowania aplikacji. Po wpisaniu numeru dotykamy **Register**.





4 Po chwili powinniśmy dostać SMS ze specjalnym kodem weryfikacyjnym. Signal automatycznie rozpozna kod i potwierdzi rejestrację.

5 Podajemy nazwę naszego profilu i jeśli chcemy – ustawiamy zdjęcie profilowe. Na koniec wybieramy **Zakończ**. Po wstępnej konfiguracji możemy ustalić, żeby Signal był naszą domyślną aplikacją do obsługi SMS-ów. Wiadomości tworzymy tak jak w większości aplikacji, dotykając symbolu długopisu u dołu ekranu. **Uwaga!** Wiadomości będą szyfrowane tylko i wyłącznie wtedy, gdy obydwie osoby uczestniczące w rozmowie korzystają z aplikacji Signal.



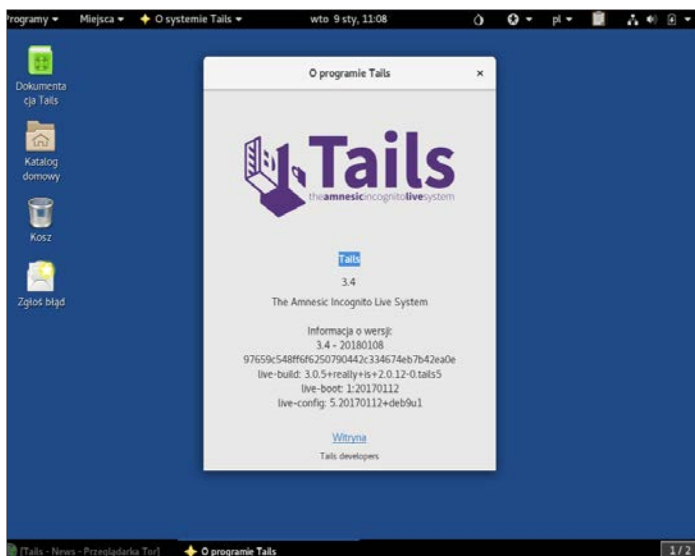
7 System Tails: całkowita anonimowość

PROGRAMY OPISANE W TYM ROZDZIALE ZNAJDZIESZ **NA DVD**

Tails to specjalny system, dzięki któremu będziemy mogli zostać anonimowi w internecie praktycznie bez żadnego wysiłku. Wbudowane w niego narzędzia i mechanizmy chronią nas przed zdradzeniem tożsamości w internecie. Przeczytajmy, jak korzystać z tego systemu i jakie ma funkcje

Czym jest Tails?

Jest to specjalny system operacyjny oparty na Linuxie, którego głównym zadaniem jest sprawienie, aby użytkownik stał się anonimowy w internecie. Sama nazwa systemu to skrót od **The Amnesic Incognito Live System**, co jest tłumaczone jako „system z amnezją działający w trybie incognito w wersji Live".



To, że system działa w wersji Live, w przypadku systemów Linux oznacza, że możemy korzystać z niego bez instalacji, startując komputer z zawierającej go bootowalnej płyty (takiej jak ta dołączona do książki) lub z pendrive'a. Po uruchomieniu Tailsa możemy pobierać pliki z internetu lub tworzyć dokumenty, jednak będą one przechowywane jedynie w pamięci podręcznej. Oznacza to, że po wyłączeniu systemu zostaną utracone, o ile nie zapiszemy ich wcześniej na innym podłączonym do

Onion Circuits

Circuit	Status
maibrunn, SecondGateToTor, Unnamed	Built
maibrunn, zwiubel, SenjakWay	Built
maibrunn, onemoretorserver1, Unnamed	Built
maibrunn, byres, Unnamed	Built
maibrunn, THOr1, LibreZone	Built
maibrunn, KingKong, niftychinchilla	Built
maibrunn, mathsgtpolitics, nikola	Built
maibrunn, isthistherealworld, KyleBroflovski	Built
maibrunn, DanWin1210, marcuse1	Built
maibrunn, morha, modio	Built

maibrunn
Fingerprint: E9025AD60D86875D5F11548D536CC6AF60F0EF5E
Published: 2018-01-09 10:51:41
IP: 179.43.188.206 (Switzerland)
Bandwidth: 11.33 Mb/s

isthistherealworld
Fingerprint: 6FAAD7CC7EBB008AEF2E5AE1BB9082CD8BD60648
Published: 2018-01-09 09:45:12
IP: 212.51.156.224 (Switzerland)
Bandwidth: 53.42 Mb/s

KyleBroflovski
Fingerprint: 335746A6DEB684FABDF3FC5835C3898F05C5A5A8
Published: 2018-01-09 12:20:23
IP: 216.218.222.14 (United States)
Bandwidth: 59.57 Mb/s

komputera nośniku zewnętrznym lub w chmurze. W przypadku systemu, który ma zapewnić anonimowość i bezpieczeństwo, jest to bardzo dobre rozwiązanie. Czasem jednak użytkownicy chcą skorzystać ze stałej przestrzeni dyskowej. W takim wypadku, jeśli mamy Tailsa na pendrivie, można skorzystać ze specjalnego trybu **persistence**, który pozwala na korzystanie z przestrzeni nośnika USB jak z dysku twardego.

Mechanizmy zapewniające anonimowość w systemie Tails

Nie bez powodu Edward Snowden zdecydował się na używanie tego systemu. Pomimo wielu audytów bezpieczeństwa, które miały wykryć słabe punkty tej dystrybucji, nieodmiennie jest ona jedną z najbezpieczniejszych. Poznajmy najważniejsze funkcje i mechanizmy, które sprawiają, że możemy być spokojni o naszą anonimowość.

■ Korzystanie z zapewniającej anonimowość sieci Tor

Nie chodzi tu tylko o przeglądarkę. Od razu po uruchomieniu systemu Tails zostaje nawiązane połączenie ze specjalną siecią Tor. Cały ruch sieciowy wszystkich usług i programów jest skierowany tylko i wyłącznie przez kanały tej sieci. W przypadku Windows, nawet jeśli korzystamy z sieci Tor, to w każdej chwili dowolna usługa systemu lub program może zażądać dostępu do internetu i tym samym zdradzić naszą anonimowość. Nic takiego nie stanie się w Tailsie.

■ Domyślnie zamknięte wszystkie niepotrzebne porty

Dzięki temu rozwiązaniu użytkownik nie jest narażony na atak z zewnątrz, gdyż wszystkie porty zostały systemowo zamknięte i nie ma możliwości zaatakowania naszego komputera przez wysyłanie żądania na jeden z portów. W momencie gdy wybrana aplikacja chce nawiązać połączenie z internetem z wykorzystaniem wybranego portu, jeśli jest uwzględniona na specjalnej liście programów, może rozpocząć komunikację, w innym przypadku nie dojdzie do nawiązania połączenia.

■ Domyślnie brak uprawnień administratora

Jest to jedno z najlepszych rozwiązań chroniących mało zaawansowanych użytkowników. Oznacza brak możliwości instalowania nowych aplikacji i programów, co jest niezwykle ważne w przypadku systemu Tails. Jak już wiemy, cały ruch sieciowy systemu jest kierowany przez sieć Tor, co jest zapewnione przez odpowiednią konfigurację wszystkich aplikacji. W przypadku gdyby użytkownik zainstalował sobie dodatkowe aplikacje i nie przekierował odpowiednio ich ruchu sieciowego, byłby narażony na ryzyko utraty anonimowości. Nie mając uprawnień administratora, użytkownik nie uruchomi też przez przypadek żadnego złośliwego kodu. (Można włączyć tryb administratora, jednak jest to wskazane tylko w wypadku zaawansowanych użytkowników).

■ Automatyczny spoofing karty sieciowej

Niezależnie od tego, czy korzystamy z połączenia przewodowego czy Wi-Fi – Tails



domyślnie zmieni adres MAC naszej karty sieciowej, dzięki czemu nie będzie można powiązać później naszego komputera z generowanym w sieci ruchem. Jest to niezwykle przydatne zwłaszcza w przypadku korzystania z sieci publicznych.



■ Zainstalowane dodatki do wielu programów

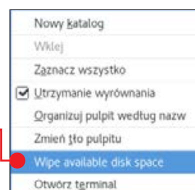
Kolejnym elementem zwiększającym bezpieczeństwo są specjalne dodatki zainstalowane w przeglądarce, klientach pocztowych, komunikatorze i innych programach użytkowych. Zapewniają one zwiększoną ochronę i umożliwiają szyfrowanie wiadomości.

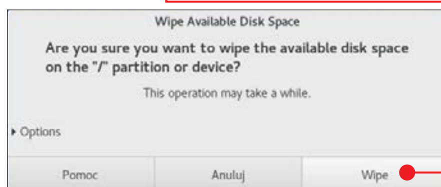
■ Zainstalowany klient OpenPGP

Dzięki niemu możliwe jest korzystanie z bardzo dobrego zabezpieczenia e-maili. Konfiguracja OpenPGP i generowanie kluczy potrzebnych do szyfrowania są bardzo proste.

■ Czyszczenie pamięci RAM i dysku

Za każdym razem, gdy zamykamy system Tails, czyści on przed zamknięciem pamięć RAM, w której były przechowywane pliki w trakcie pracy w wersji Live. Dzięki temu nie jest możliwe sprawdzenie, nad czym pracowaliśmy. Dodatkowo z poziomu systemu możemy w każdej chwili sami zarządzić czyszczenie wolnej przestrzeni dyskowej, co może być przydatne, gdy korzystamy z nośnika USB. Klikamy prawym przyciskiem myszy na pulpit i na **Wipe available disk space**, a następnie w kolejnym oknie na **Wipe**.



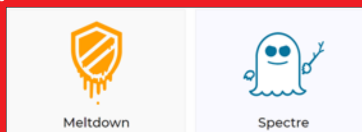


■ Szyfrowanie dysków

W systemie Tails mamy możliwość zaszyfrowania nośnika USB lub dysku zewnętrznego za pomocą LUKS, czyli standardu szyfrowania przestrzeni dyskowej dla systemu Linux. Zapewnia to bardzo wysoki poziom bezpieczeństwa, a zarazem nie wpływa znacząco na wydajność nośników. Jest to szczególnie przydatne przy korzystaniu z rozszerzonej przestrzeni użytkownika (persistence).

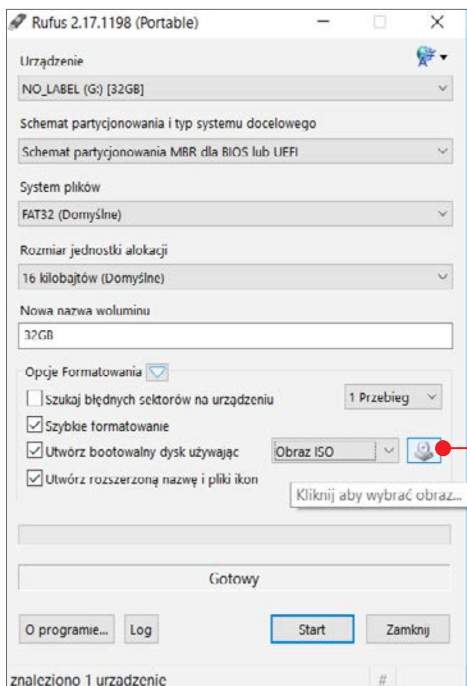
WAŻNE AKTUALIZACJE SYSTEMU

Aktualizacje do Tailsa publikowane są regularnie, najczęściej duże zmiany wprowadzane są raz lub dwa razy do roku, znacznie częściej pojawiają się aktualizacje naprawiające błędy lub usuwające zagrożenia. Jedną z nich była aktualizacja z 10 stycznia 2018 roku do wersji 3.4 – nie wniosła żadnych nowych funkcji do systemu, a jedynie zaktualizowała jego zabezpieczenia przed zagrożeniami **Meltdown** i **Spectre**. To ważne, bo są to zagrożenia, które mogą doprowadzić do dużych strat w każdym systemie.



Tworzymy nośnik USB z systemem Tails

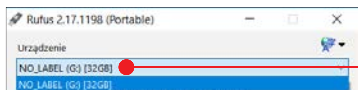
Korzystając z dołączonej do książki płyty, możemy uruchomić z niej system Tails i korzystać z jego możliwości. Jednak możemy również utworzyć samemu bootowalny nośnik USB. Takie rozwiązanie oprócz tego, że daje nam kilka nowych możliwości, pozwala na korzystanie z systemu z większą wydajnością (zależną od wydajności nośnika USB). Jeśli korzystamy z bardzo wydajnego nośnika typu USB 3.0, może okazać się, że taki system w wersji Live będzie pracował szybciej niż system Windows zainstalowany na dysku twardym. **Uwaga!** Aby wykonać tę wskazówkę, potrzebny jest pendrive o pojemności minimum 4 GB (jeśli chcemy korzystać z persistence, zalecane jest przynajmniej 8 GB). **Na pendrivie nie powinno być ważnych danych – zostaną one całkowicie usunięte.**



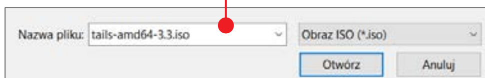
1 Pobieramy na dysk z KŚ+ (www.ksplus.pl) lub kopiujemy z płyty DVD dołączonej do książki obraz: **tails-amd64-3.4.iso**.

2 Następnie uruchamiamy program **Rufus**, który umożliwia tworzenie bootowalnych nośników (znajdziemy go na płycie).

3 Podłączamy pendrive do komputera, na górze okna programu w polu **Urządzenie** powinniśmy zobaczyć nasz nośnik.



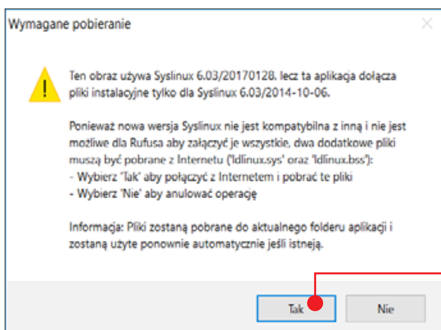
4 Następnie klikamy na ikonę napędu CD/DVD i wskazujemy obraz ISO Tailsa zapisany na dysku. Klikamy na **Otwórz**.

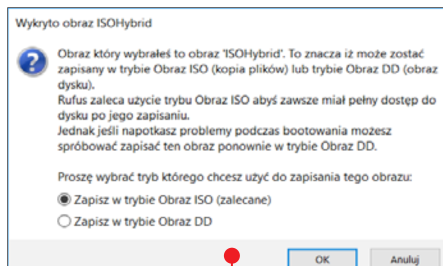


5 Na dole okna programu pojawi się informacja o aktualnie załadowanym obrazie. Wystarczy teraz kliknąć na **Start**.



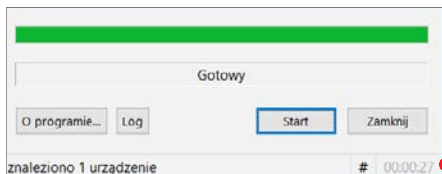
6 Następnie musimy kliknąć na **Tak**, żeby pobrać z internetu dodatkowe aktualne pliki instalacyjne.





7 Teraz pojawi się okno z informacją o obrazie ISOHybrid. Pozostawiamy domyślne ustawienia i klikamy na **OK**.

8 Pozostaje nam jeszcze tylko potwierdzenie informacji o formatowaniu i po chwili będziemy mogli korzystać z nowego bootowalnego nośnika. W naszym przykładzie cały proces trwał tylko 27 sekund.



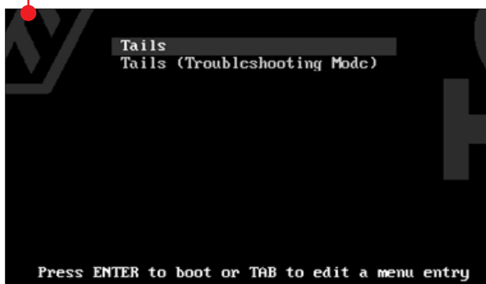
Uruchamiamy Tails – krok po kroku

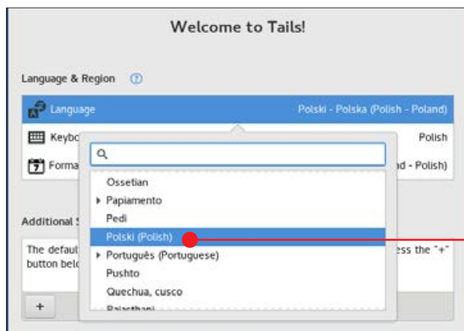
W zależności od tego, czy zamierzamy uruchomić system Tails z płyty czy z pendrive'a, procedura może się trochę różnić, ale wygląda podobnie.

1 Umieszczamy nośnik w komputerze. Następnie restartujemy komputer i podczas uruchamiania przechodzimy do ustawień BIOS-u lub Boot Menu, najczęściej trzeba w tym celu nacisnąć klawisze F2, F8, F10 lub delete. Następnie wybieramy nośnik startowy – DVD lub USB.

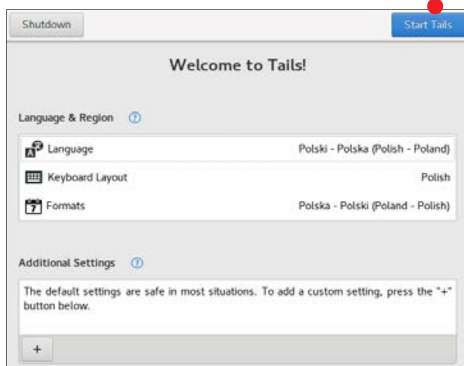
2 Teraz powinniśmy zobaczyć ekran startowy systemu Tails. Możemy poczekać trzy sekundy lub nacisnąć enter.

3 Następnie pojawi się okno logowania do systemu. Zanim przejdziemy dalej, klikamy na **Language** na środku ekranu i wybieramy z listy **Polski (Polish)**.



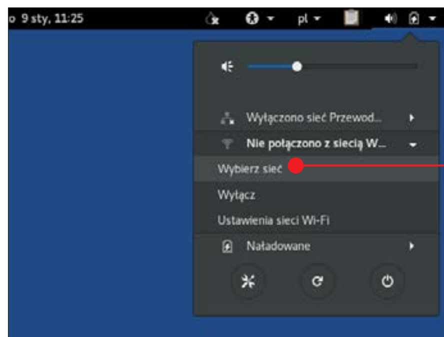


4 Teraz możemy przejść do systemu, klikając na **Start Tails**.



Łączymy się z internetem

Jeśli korzystamy z połączenia przewodowego, system automatycznie powinien skonfigurować połączenie i uzyskać dostęp do internetu. W przypadku gdy chcemy połączyć się z siecią Wi-Fi, musimy wykonać kilka prostych kroków.

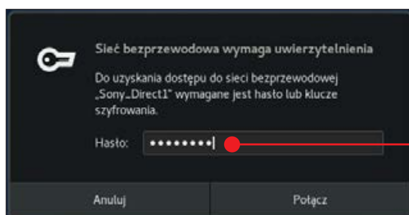


1 Klikamy w górnym prawym rogu ekranu na strzałkę, a następnie na **Nie połączono z siecią Wi-Fi** i na **Wybierz sieć**.



2 Teraz klikamy na sieć, z którą chcemy nawiązać połączenie, i na **Połącz**.

3 Następnie podajemy hasło dostępu do sieci Wi-Fi i znowu klikamy na **Połącz**. Po chwili bezpieczne połączenie z siecią Tor zostanie nawiązane i będziemy mieli dostęp do internetu.

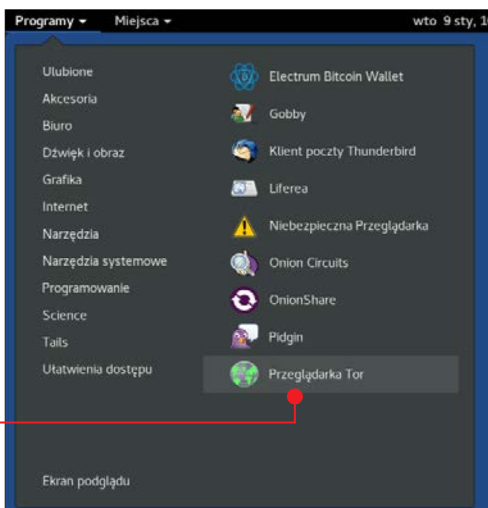


Korzystamy z dostępnych programów

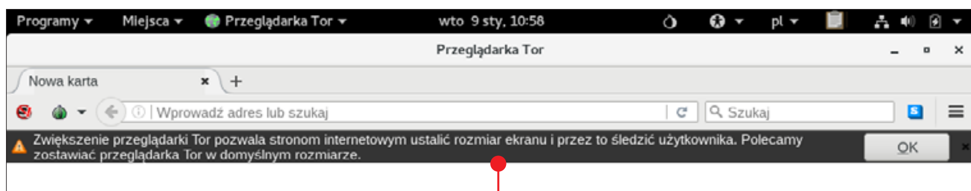
Tails ma wbudowane programy, które pozwolą nam na bezpieczne i anonimowe korzystanie z internetu. Jednym z nich jest Tor Browser, który powinien od razu przy starcie systemu wybrać odpowiedni obwód w sieci Tor. Zaleca się, by po uruchomieniu systemu połączyć się z internetem i po kolei sprawdzić, czy wybrane programy i funkcje systemu działają, ponieważ to właśnie od nich zależeć będzie nasze bezpieczeństwo.

Tor Browser

1 Klikamy w górnym prawym rogu na **Programy**, a następnie najeżdżamy kursorem na **Internet** i klikamy na **Przeglądarka Tor**.



2 Od razu przy uruchomieniu zostaniemy poinformowani, że najlepiej nie zmieniać

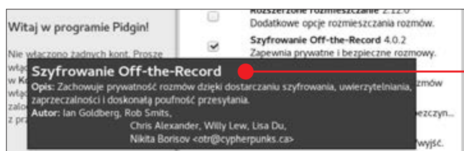


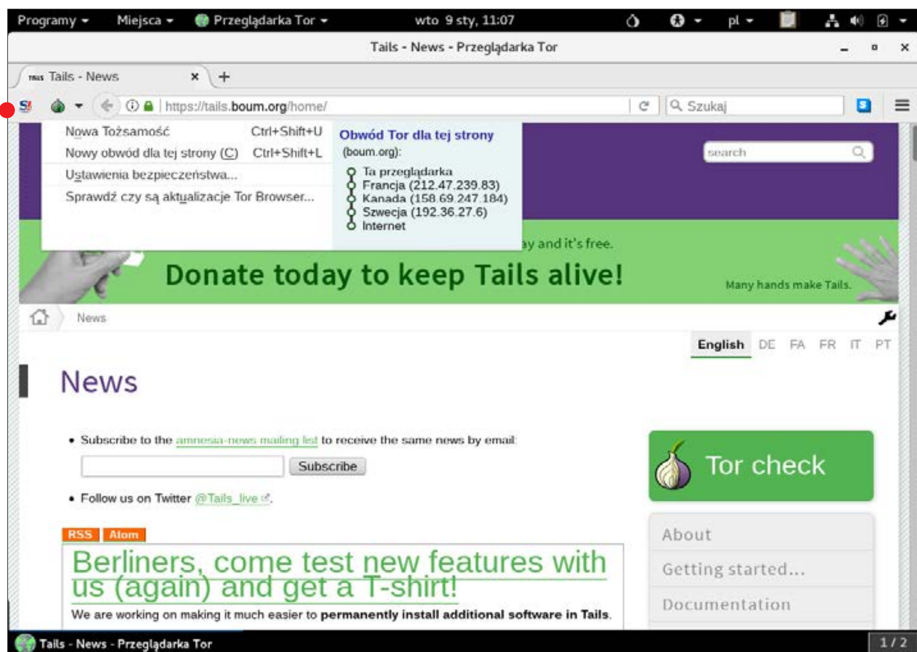
rozmiaru okna przeglądarki Tor, gdyż może to ułatwić wykrycie i śledzenie nas w internecie.

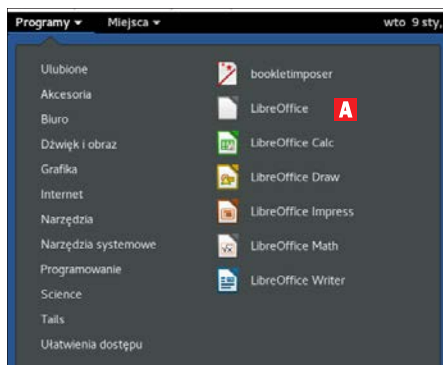
3 Następnie klikamy na ikonę cebuli na górnym pasku i upewniamy się, że nie ma żadnego ostrzeżenia. Po prawej stronie powinniśmy zobaczyć wybrany dla nas bezpieczny obwód. Jeśli wszystko wygląda podobnie jak w naszym przykładzie, możemy zacząć korzystanie z przeglądarki.
Warto dodać, że wersja przeglądarki Tor Browser w systemie Tails to specjalna zmodyfikowana wersja, która jest wyposażona w takie dodatki, jak: **NoScript**, **HTTPS Everywhere**, **Torbutton** i inne. Dzięki nim możemy czuć się bezpiecznie.

Pidgin

Jest to darmowy komunikator, który pozwoli nam na bezpieczną i anonimową komunikację ze znajomymi. Pozwala na integrację kont z innych komunikatorów, jak ICQ, Jabber, Gadu-Gadu, IRC i inne. Umożliwia też przesyłanie plików czy sprawdzanie pisowni. W wersji dla systemu Tails Pidgin ma od razu zainstalowany dodatek **Szyfrowanie Off-the-Record**, który pozwala na prowadzenie zaszyfrowanych i bezpiecznych rozmów.





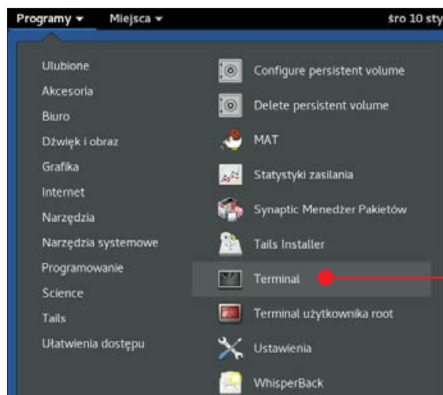


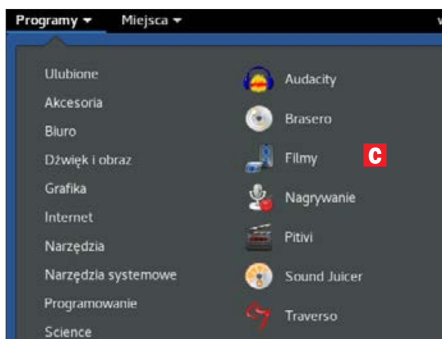
Inne programy

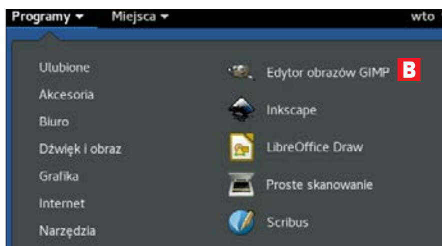
Do dyspozycji mamy praktycznie komplet potrzebnych na co dzień podstawowych programów, między innymi pakiet biurowy LibreOffice **A**, edytor graficzny GIMP **B**, programy do odtwarzania filmów i muzyki **C** czy do wyświetlania zdjęć. Dodatkowo możemy korzystać również z programów do wypalania płyt, nagrywania dźwięku i filmów. Wszystko to sprawia, że przy zachowaniu całkowitej anonimowości możemy korzystać z większości funkcji normalnego systemu operacyjnego.

PWGen

Jest to bardzo prosty program działający tylko i wyłącznie w terminalu. Służy on do generowania pseudolosowych haseł, które są trudne do złamania. Większość użytkowników korzysta z bardzo prostych haseł, które uwzględniają ich imiona, daty urodzin ich albo ich bliskich. Dzięki PWGen będziemy mogli tworzyć i wykorzystywać bardzo silne, trudne do złamania hasła.







1 Klikamy w górnym lewym rogu na **Programy**, następnie najeżdżamy kursorem na **Narzędzia systemowe** i klikamy na **Terminal**.

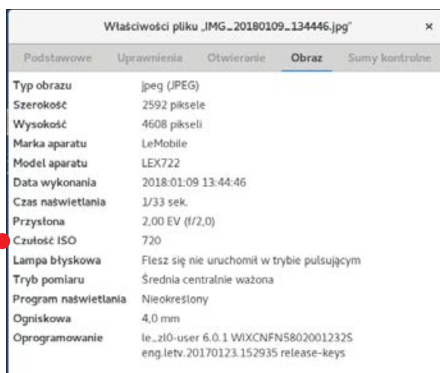
2 Teraz wystarczy wpisać i zatwierdzić klawiszem enter komendę: **pwgen -1 -c -n -y 10**.

3 Dzięki temu zostanie wygenerowane hasło składające się z 10 znaków, zawierające przynajmniej jedną dużą literę i jeden znak specjalny. Możliwości generowania haseł jest znacznie więcej. Jeśli chcemy je poznać, wystarczy wpisać w Terminalu i zatwierdzić komendę **pwgen --help**.

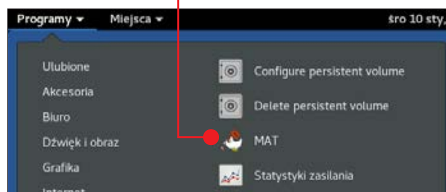


MAT

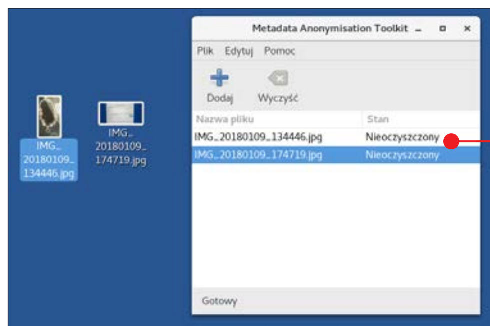
Nazwa programu MAT to skrót od **Metadata Anonymisation Toolkit**. To kolejna unikalna aplikacja w systemie Tails. Służy głównie do przerabiania plików multimedialnych, a konkretnie ich metadanych. Zawsze gdy robimy zdjęcie, zachowywane są metadane, czyli informacje na temat aparatu, jakim je wykonaliśmy, godziny i daty, ustawień przysłony, pozycji GPS i wiele innych. Jeśli mamy zamiar umieścić zdjęcie w internecie, możemy najpierw wyczyścić tego typu informacje, dzięki czemu nikt nie będzie wiedział, kiedy i gdzie oraz jakim urządzeniem zostało ono wykonane.



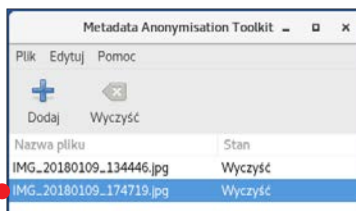
1 Klikamy w górnym lewym rogu na **Programy**, następnie najeżdżamy kursorem na **Narzędzia systemowe** i klikamy na pozycję **MAT**.



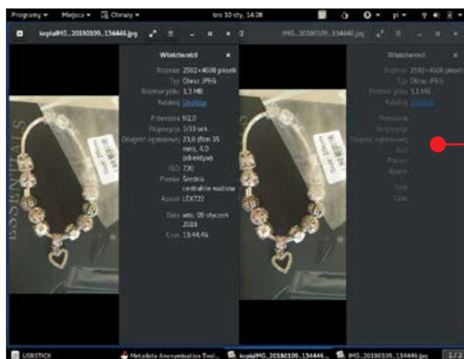
2 Następnie przeciągamy wybrane zdjęcia, których dane chcemy wyczyścić, do okna programu. Zostaną one dodane i pojawi się przy nich status **Nieoczyszczony**.



3 Teraz wystarczy kliknąć na **Wyczyść** na górnym pasku okna programu. Po chwili zdjęcie zostanie oczyszczone z metadanych, czynność musimy powtórzyć dla każdego zdjęcia osobno.



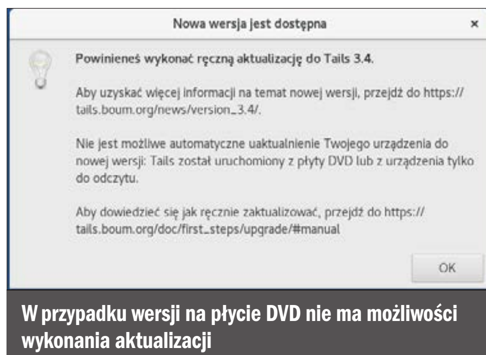
4 Po przejściu do właściwości wyczyszczonych zdjęć przekonamy się, że metadane zostały usunięte i nasze zdjęcie jest anonimowe, a jednocześnie wyświetla się zupełnie normalnie.



Dodatkowym plusem takiego rozwiązania jest możliwość zredukowania rozmiaru zdjęć przy zachowaniu ich jakości. Średnio na każdym zdjęciu jest to oszczędność 0,2 MB.

Aktualizacja systemu

Jeśli będziemy używać systemu Tails przez dłuższy czas, może okazać się, że pojawią się aktualizacje. Jeżeli korzystamy z płyty DVD dołączonej do książki, nie będziemy mogli wykonać aktualizacji, możemy ewentualnie pobrać zaktualizowaną wersję systemu z internetu i wypalić nową płytę. Jeśli jednak korzystamy z pamięci USB, możemy, a nawet powinniśmy przeprowadzić aktualizację bezpośrednio po uruchomieniu systemu Tails. Nie musimy konfigurować żadnej dodatkowej przestrzeni.



W przypadku wersji na płycie DVD nie ma możliwości wykonania aktualizacji

Aktualizujemy Tails na USB

1 Po uruchomieniu systemu i połączeniu się z internetem po chwili pojawi się informacja o aktualizacji (jeśli taka jest dostępna).

2 Klikamy na **Aktualizuj teraz**. Rozpocznie się pobieranie aktualizacji.

Dostępna aktualizacja

Powinieneś zaktualizować system do Tails 3.4.

Aby uzyskać więcej informacji na temat nowej wersji, idź do https://tails.boum.org/news/version_3.4/.

Zaleca się zamknięcie wszystkich otwartych aplikacji w czasie aktualizacji. Pobieranie aktualizacji może zająć sporo czasu, od kilku minut do nawet kilku godzin.
Połączenie sieciowe zostanie wyłączone po pobraniu aktualizacji.

Rozmiar pliku do pobrania: 176,41MiB

Czy chcesz teraz zaktualizować system?

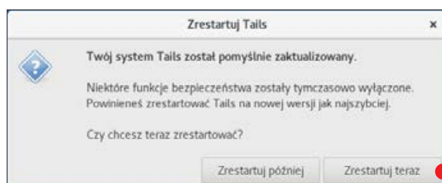
Aktualizuj później | Aktualizuj teraz

3 Po pobraniu automatycznie w tle rozpocznie się instalacja. Następnie pojawi się komunikat informujący o konieczności ponownego uruchomienia systemu. Klikamy na **Zrestartuj teraz**.

Pobierania aktualizacji

Trwa pobieranie aktualizacji do Tails 3.4...

4 Gdy system uruchomi się ponownie, będzie już aktualny. Jest to jedno z najlepszych rozwiązań aktualizacji, zwłaszcza w systemie typu live.



Przestrzeń dla użytkownika

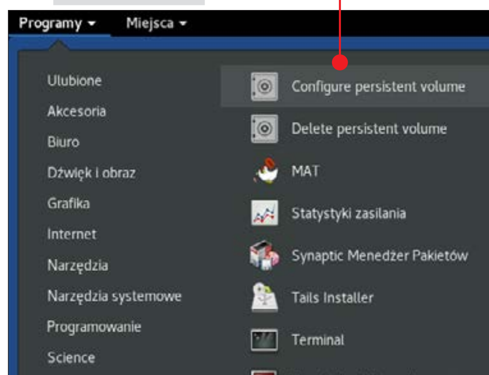
Tails umożliwia nam skonfigurowanie na pendrivie specjalnej przestrzeni dyskowej zabezpieczonej hasłem, na której będziemy mogli przechowywać nasze pliki, a dodatkowo pozwoli to znacznie łatwiej korzystać z różnych funkcji systemu, na przykład szyfrowania wiadomości, do czego potrzeba w pełni skonfigurowanego klienta poczty. Po utworzeniu tej specjalnej dodatkowej przestrzeni o nazwie **persistent volume** będziemy mieli możliwość przechowywania również plików konfiguracyjnych.

Uwaga! Ta opcja jest możliwa do skonfigurowania tylko w przypadku korzystania z pendriv'a lub dysku zewnętrznego.

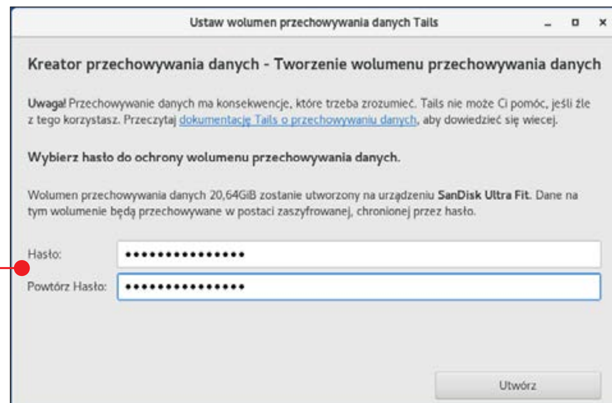
1 Musimy utworzyć bootowalny nośnik USB z Tailsem (patrz wcześniejsze porady).

2 Uruchamiamy system Tails i przechodzimy do pulpitu.

3 Klikamy w górnym lewym rogu na **Programy**, najeżdżamy kursorem na **Narzędzia systemowe** i klikamy na **Configure persistent volume**.



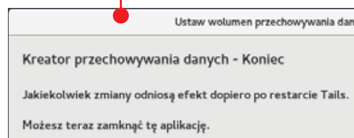
4 Uruchomiony zostanie kreator przechowywania danych. Na pierwszym ekranie podajemy hasło, które będzie służyło do ochrony naszych danych. U dołu okna klikamy na **Utwórz**.



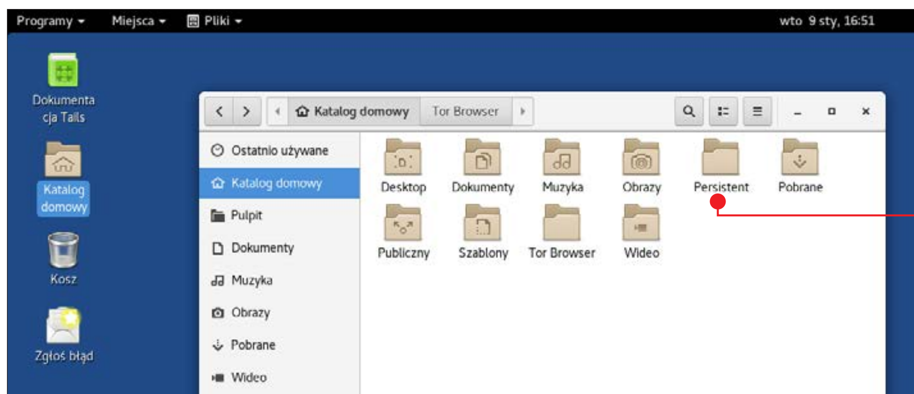


5 W przypadku nośnika o rozmiarze 32 GB można utworzyć tylko 20,64 GB miejsca na dane użytkownika. Zaznaczamy, z jakich opcji chcemy korzystać i jakie pliki będą mogły być przechowywane w nowo utworzonej przestrzeni. Po wybraniu odpowiednich opcji klikamy na polecenie **Zapisz**.

6 Następnie zamykamy kreator przechowywania danych i ponownie uruchamiamy system Tails.



7 Przy ponownym uruchomieniu komputera wystarczy na ekranie logowania systemu Tails w polu **Encrypted Persistent Storage** podać nasze hasło i kliknąć na **Unlock**. Jeśli wpisane hasło jest poprawne, przestrzeń dyskowa zostanie odblokowana.





8 Klikamy na **Start Tails** i zaczynamy korzystanie z systemu i naszej przestrzeni.

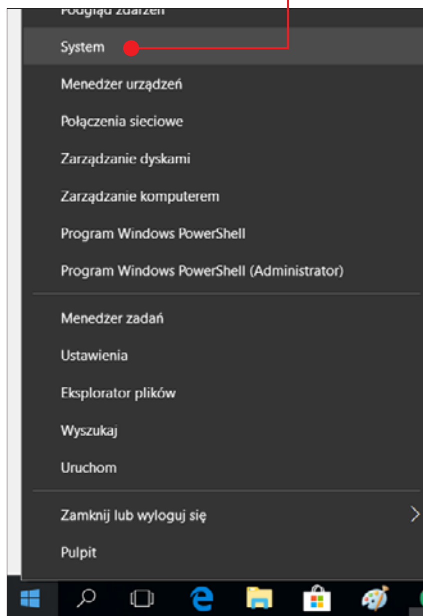
9 Dostęp do niej uzyskamy, klikając na pulpicie na **Katalog domowy**, **Persistent**. Wszystkie pliki w tym katalogu będą zaszyfrowane i nie będą automatycznie usuwane przy kolejnych uruchomieniach systemu. Możemy także korzystać z systemu Tails bez tej dodatkowej przestrzeni – wystarczy nie odblokowywać chronionego zasobu w oknie logowania i po prostu przejść do systemu.

VirtualBox i Tails DLA ZAAWANSOWANYCH

Wirtualne środowisko do korzystania z systemu Tails może przydać się wielu użytkownikom, którzy nie chcą wyłączać systemu Windows i uruchamiać komputera z nośnika bootowalnego, aby skorzystać z bezpiecznego środowiska. Konfiguracja tego rozwiązania jest wbrew pozorom dość prosta. Należy jednak pamiętać o ograniczeniach sprzętowych naszych komputerów. W celu uruchomienia wirtualnego środowiska musimy „podzielić się” z nim zasobami naszego komputera, pamięcią RAM, przestrzenią dyskową, procesorami, kartą graficzną itp. Poza tym nasz procesor musi obsługiwać technologię wirtualizacji. Jeśli nie wiemy, czy tak jest, możemy sprawdzić, czy nasza jednostka obliczeniowa ma wsparcie dla technologii **AMD-V** lub **Intel VT-x**, które służą do wirtualizacji fizycznych maszyn (patrz kolejna strona). Potrzebna nam też będzie aplikacja zarządzająca, czyli na przykład **VirtualBox** (znajdziemy go na płycie dołączonej do książki).

Sprawdzamy wsparcie dla technologii wirtualizacji

1 Klikamy prawym przyciskiem myszy na menu **Start** i na **System**.



2 Następnie w oknie po prawej stronie znajdziemy informację o naszym procesorze.

Procesor	Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz 2.60 GHz
Zainstalowana pamięć RAM	24,0 GB (23,8 GB usable)

3 Teraz w wyszukiwarce lub na stronie producenta wpisujemy model proceso-

Technologie zaawansowane	
Technologia Intel® Turbo Boost ‡	2.0
Technologia Intel® vPro™ ‡	Nie
Technologia Intel® Hyper-Threading ‡	Tak
Technologia Intel® Virtualization (VT-x) ‡	Tak
Technologia Intel® Virtualization for Directed I/O (VT-d) ‡	Tak
Technologia Intel® VT-x with Extended Page Tables (EPT) ‡	Tak
Intel® TSX-NI	Nie
Intel® 64 ‡	Tak

ra i szukamy informacji na temat technologii wirtualizacji. W przypadku firmy **Intel** informację tę znajdziemy w kategorii **Technologie zaawansowane**, **Technologia Intel® Virtualization (VT-x)** – nasz procesor musi mieć status **Tak**.

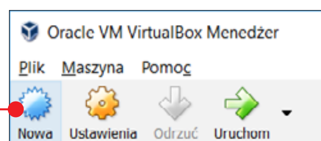
WYMAGANA ILOŚĆ PAMIĘCI RAM

Jeśli zamierzamy wirtualizować środowisko 64-bitowe na naszym komputerze w systemie Windows 10, powinniśmy mieć przynajmniej 8 GB pamięci RAM. Ogólnie obowiązuje zasada – im więcej, tym lepiej. Mała ilość wolnej pamięci RAM będzie skutkować spowolnioną pracą obydwu systemów.

Tworzymy wirtualną maszynę z systemem Tails

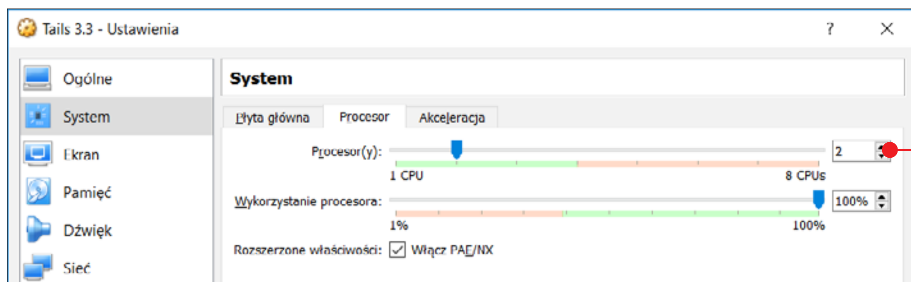
1 Najpierw instalujemy VirtualBox. Najlepiej zdecydować się na domyślną instalację wraz ze wszystkimi sterownikami sieciowymi.

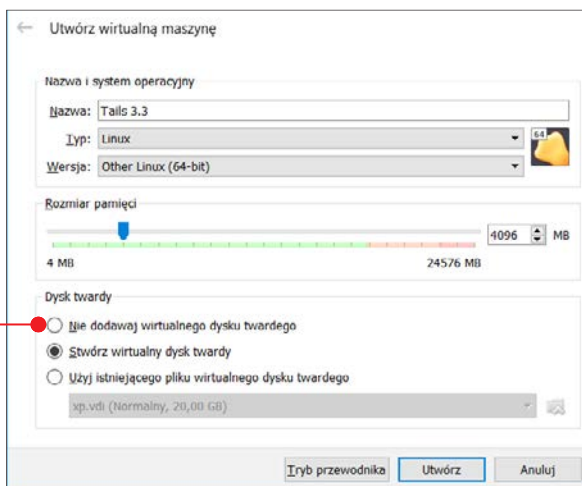
2 Uruchamiamy program VirtualBox i w górnym lewym rogu klikamy na **Nowa**.

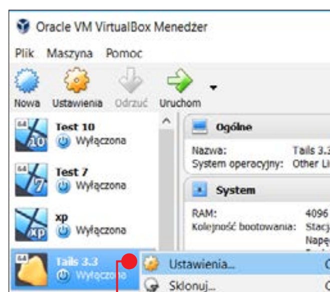


3 Teraz nadajemy nazwę naszej wirtualnej maszynie. Wybieramy z rozwijanych list opcję **Linux**, **Other Linux (64-bit)**, określamy ilość przysługującej pamięci RAM (dla optymalnej pracy – 2 GB) i zaznaczamy opcję **Nie dodawaj wirtualnego dysku twardego** – ponieważ będziemy korzystać z systemu w wersji Live. Klikamy na **Utwórz**.

4 Nasza nowa maszyna pojawi się w menedżerze VirtualBoxa w oknie po lewej







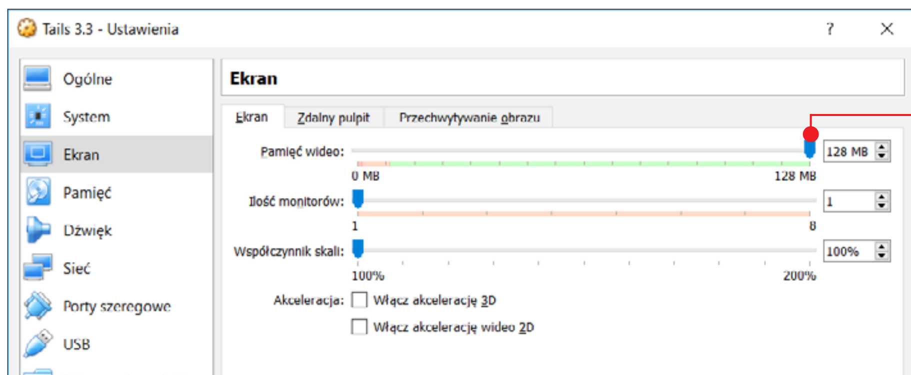
stronie. Klikamy na nią prawym przyciskiem myszy, a następnie na **Ustawienia** ●.

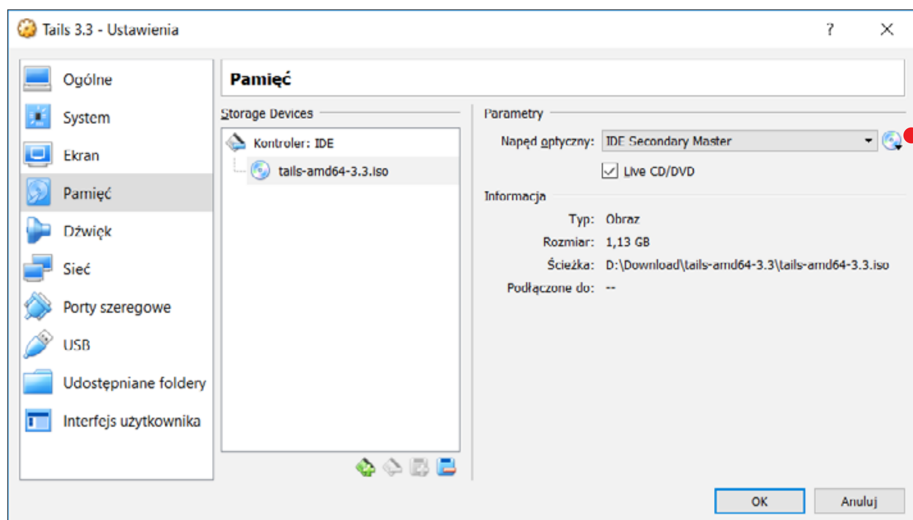
5 Teraz po lewej stronie klikamy na **System**, a później po prawej na **Procesor**.

Jeśli mamy do dyspozycji osiem procesorów, możemy spokojnie wybrać **2** ● lub **4** i przejść do kategorii **Ekran**.

6 Przesuwamy suwak przy opcji **Pamięć wideo** do końca w prawą stronę ● i po lewej stronie klikamy na **Pamięć**.

7 Po prawej stronie klikamy na napęd CD pod kontrolerem IDE, zaznaczamy opcję

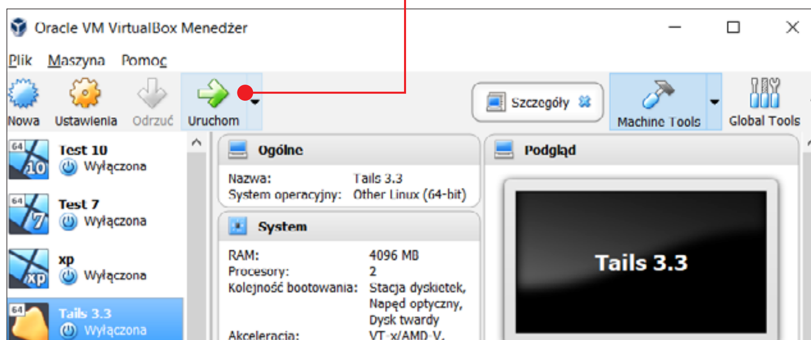




Live CD/DVD, klikamy na ikonę płyty CD, nawigujemy do obrazu systemu Tails i go wybieramy. Na koniec klikamy na **OK**.

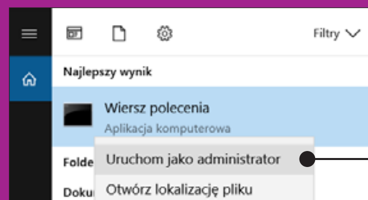
8 Teraz możemy uruchomić naszą nową wirtualną maszynę, wystarczy wybrać ją z listy i kliknąć na **Uruchom**.

Korzystanie z systemu Tails w maszynie wirtualnej wygląda tak samo jak w przypadku uruchamiania Tailsa na komputerze.
Pod względem bezpieczeństwa jest to rozwiązanie pośrednie. Jest znacznie bezpieczniejszym wyjściem niż korzystanie z samego systemu Windows, jednak nie zapewnia nam gwarantowanego bezpieczeństwa, tak jak Tails działający z pamięci USB lub płyty. Pomimo zabezpieczenia komunikacji i zapewnienia anonimowości naszą tożsamość w internecie nadal może narazić system Windows, który w tym samym czasie może zażądać aktualizacji, podobnie jak inne programy.
Jest to jednak wygodny sposób korzystania z anonimowych narzędzi. Sam system Tails jest w stanie wykryć to, że został uruchomiony jako maszyna wirtualna i po włączeniu go w tym środowisku pokazuje komunikat, który dodatkowo informuje nas o zagrożeniach wynikających z korzystania z tego systemu w ten sposób. Zdecydowana większość użytkowników nie ma się jednak czego obawiać.



HYPER-V A VIRTUALBOX

Dość częstym problemem użytkowników po raz pierwszy używających programu VirtualBox jest brak możliwości skonfigurowania maszyn 64-bitowych. Przyczyną trudności jest działanie specjalnego narzędzia instalowanego w systemach Windows 8 i 10 – **Hyper-V**. To oprogramowanie, które w Windows odpowiada za tworzenie wirtualnych maszyn i przy starcie systemu automatycznie zajmuje sterownik procesora odpowiedzialny za wirtualizację.
Możemy rozwiązać ten problem na dwa sposoby. Pierwszy to całkowite usunięcie narzędzia Hyper-V z systemu Windows lub zablokowanie jego startu w systemie. Druga opcja jest prostsza i pozwala w każdej chwili cofnąć zmiany.



1 Uruchamiamy Wiersz polecenia jako administrator.

2 Następnie wpisujemy komendę: **bcdedit / set hypervisorlaunchtype off** i zatwierdzamy klawiszem enter.

Administrator: Wiersz polecenia

```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\WINDOWS\system32>bcdedit /set hypervisorlaunchtype off
Operacja ukończona pomyślnie.
```

3 Po ponownym uruchomieniu komputera powinniśmy móc tworzyć 64-bitowe maszyny wirtualne.

4 Jeśli chcemy cofnąć zmiany, wystarczy ponownie wykonać krok **1**, wpisać komendę: **bcdedit / set hypervisorlaunchtype auto** i zatwierdzić klawiszem enter.

```
C:\WINDOWS\system32>bcdedit /set hypervisorlaunchtype auto
Operacja ukończona pomyślnie.

C:\WINDOWS\system32>
```

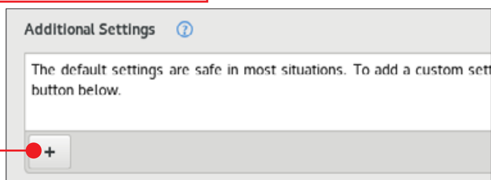
Tryb administratora

DLA ZAAWANSOWANYCH

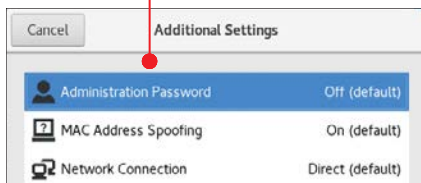
Zdarza się, że użytkownicy korzystający z systemu Tails chcą zainstalować ulubiony program lub zmienić jakieś systemowe ustawienia. Domyślnie nie jest to możliwe, bo wyłączony jest tryb administratora, ponieważ mało doświadczony użytkownik, używając go, mógłby przez przypadek zdradzić swoją anonimowość. Uruchomienie trybu administratora nie jest trudne, jednak pamiętajmy, że jeśli chcemy nadal pozostać anonimowi, musimy używać go odpowiedzialnie.

Uruchamiamy tryb administratora

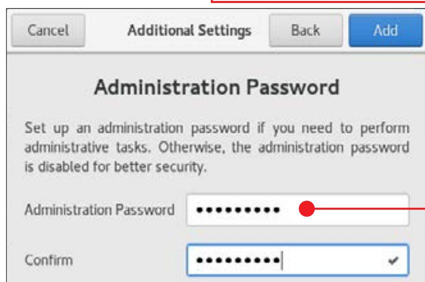
1 Po uruchomieniu systemu Tails na ekranie logowania klikamy na symbol **+** w lewym dolnym rogu.



2 Następnie klikamy na **Administration Password** ●.



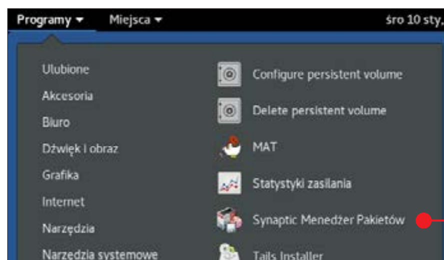
3 Wpisujemy i potwierdzamy hasło, jakie nam odpowiada ●, i klikamy na **Add**.



4 Teraz możemy kliknąć na **Start Tails** i korzystać z praw administratora za każdym razem, gdy będziemy chcieli.

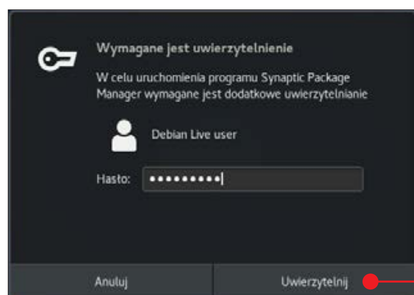
Instalujemy i aktualizujemy programy

Tails oparty jest na systemie Debian i obsługuje jego paczki instalacyjne, dlatego też do naszej dyspozycji jest wiele różnych programów i aplikacji.
Jest w nim też na szczęście centrum oprogramowania, z którego z łatwością można dodawać nowe programy – nie trzeba robić tego ręcznie za pomocą terminalu. W systemie Tails możemy też aktualizować wybrane pakiety.

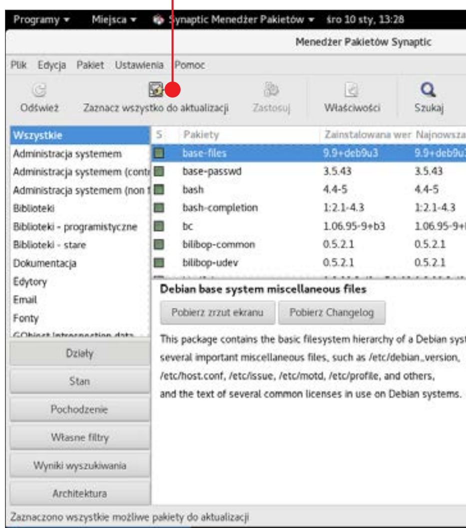


1 Klikamy w górnym lewym rogu na **Programy**, następnie najeżdżamy na **Narzędzia systemowe** i klikamy na **Synaptic Menedżer Pakietów** ●.

2 Teraz musimy podać utworzone na początku sesji hasło administratora i kliknąć na **Uwierzytelnij** ●.



3 Potem możemy kliknąć na opcję **Zaznacz wszystko do aktualizacji** ●, a następnie na **Zastosuj**.

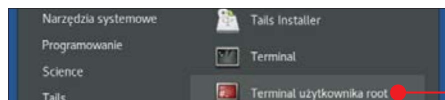


4 W ten sposób możemy mieć zawsze aktualne narzędzia i programy.
Więcej na temat instalacji dodatkowych programów przeczytamy na stronie **https://tails.boum.org**.

Macchanger

Jest to specjalny program, z którego możemy korzystać poprzez terminal. Pozwala on na zmianę adresu MAC naszej karty sieciowej. Jest to niezwykle przydatna funkcja, zwłaszcza gdy korzystamy z internetu poprzez sieci publiczne. Dzięki temu nie zostaną zapisane logi uwzględniające unikalny adres MAC naszej karty sieciowej, a jedynie nadpisane przez nas wymyślone wartości. Musimy jednak zmienić adres MAC, zanim połączymy się z siecią. Warto pamiętać, że pomimo włączenia domyślnego spoofingu (fałszowania) karty sieciowej zmiana co jakiś czas w trakcie pracy adresu MAC może zwiększyć nasze bezpieczeństwo, gdyż w sieci nasz komputer będzie widoczny jako nowe urządzenie. Zatem nawet jeśli generujemy duży ruch, to gdy zostanie rozbity na kilka adresów MAC, trudniej będzie nas wykryć. **Uwaga! Adres MAC zmieniamy tylko wtedy, gdy nie jesteśmy połączeni z żadną siecią.**

1 Klikamy na **Programy**, następnie najeżdżamy kursorem na **Narzędzia użytkowe** i klikamy na **Terminal użytkownika root**.



2 Teraz podajemy hasło administratora i klikamy na **Uwierzytelnij** (patrz punkt **2** na stronie obok). Pojawi się okno terminalu.

3 W terminalu wpisujemy komendę **ip a** i zatwierdzamy klawiszem enter. Pojawią się wszystkie interfejsy sieciowe naszego komputera. Jeśli korzystamy z sieci bezprzewodowej, interesuje nas szczególnie nazwa interfejsu **[wlan0]**, w zależności od komputera cyfra może być inna.

```
Terminal
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
root@amnesia:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
oup default qlen 1000
    link/ether 08:00:27:d7:4e:ce brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST> mtu 1500 qdisc mq state DOWN group
1000
    link/ether 7a:df:e8:ec:8c:f2 brd ff:ff:ff:ff:ff:ff
root@amnesia:~#
```

4 Następnie upewniamy się, czy dany interfejs jest dezaktywowany, wpisując komendę **ip link set dev wlan0 down**, i zatwierdzamy klawiszem enter.

```
Terminal
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
root@amnesia:~# ip link set dev wlan0 down
root@amnesia:~#
```

5 Wpisujemy i zatwierdzamy komendę **macchanger -s wlan0** (wlan0 jest naszym przypisanym interfejsem odczytanym w kroku **3**). Jeśli pojawi się adres MAC, to znaczy, że możemy przystąpić do jego zmiany.

```
Terminal
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
root@amnesia:~# ip link set dev wlan0 down
root@amnesia:~# macchanger -s wlan0
Current MAC:   4e:7f:42:83:4e:6c (unknown)
Permanent MAC: 18:d6:c7:0b:cc:b4 (unknown)
root@amnesia:~#
```

6 Możemy ręcznie wprowadzić nowy adres MAC lub skorzystać z funkcji tworzenia losowego adresu. Druga opcja jest znacznie szybsza. Wprowadzamy i zatwierdzamy komendę **macchanger -r wlan0**. Pojawi się informacja o nowo przypisanym adresie MAC.

7 Po zakończeniu procesu aktywujemy interfejs, wprowadzając i zatwierdzając komendę **ip link set dev wlan0 up**.

```
Termin
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
root@amnesia:~# ip link set dev wlan0 down
root@amnesia:~# macchanger -s wlan0
Current MAC:   4e:7f:42:83:4e:6c (unknown)
Permanent MAC: 18:d6:c7:0b:cc:b4 (unknown)
root@amnesia:~# macchanger -r wlan0
Current MAC:   4e:7f:42:83:4e:6c (unknown)
Permanent MAC: 18:d6:c7:0b:cc:b4 (unknown)
New MAC:       02:47:dc:06:0c:7a (unknown)
root@amnesia:~#
```



Szyfrowanie smartfona z Androidem

UWAGA!
W różnych wersjach Androida szyfrowanie może wyglądać inaczej.

Dbając o bezpieczeństwo i prywatność, skupiamy się głównie na naszych komputerach i laptopach. Warto jednak pamiętać, że urządzenia mobilne często mają w pamięci więcej wrażliwych informacji. SMS-y, MMS-y, kontakty, zdjęcia, filmy, ważne pliki, dane dostępu do kont, hasła do sieci i wiele innych. Dlatego warto zadbać o bezpieczeństwo, szyfrując nasze urządzenie.
W przypadku systemu Android jest to dosyć proste, ponieważ narzędzia potrzebne do zaszyfrowania całego urządzenia są już wbudowane w system i gotowe do użycia. Różnice zależą od wersji systemu zainstalowanego na naszym urządzeniu, a także od modelu smartfona, jednak nie powinno to stanowić problemu.

Uwaga! Przed rozpoczęciem procesu upewnijmy się, że nasze urządzenie jest naładowane, podłączmy je do ładowania. Pierwszy start po zaszyfrowaniu może być wolniejszy. Samo szyfrowanie urządzenia nie powinno negatywnie wpłynąć na jego osiągi.

1 Przechodzimy do ustawień naszego urządzenia.

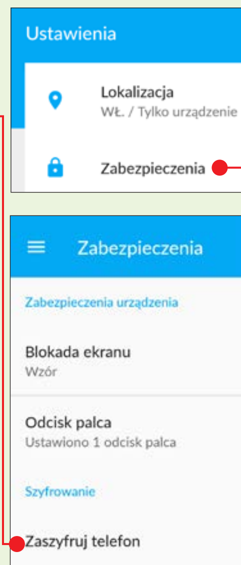
2 Naciskamy kategorię **Zabezpieczenia** (lub jej odpowiednik).

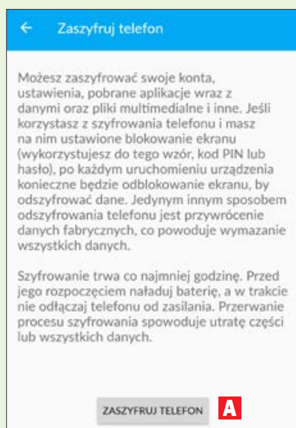
3 Następnie naciskamy opcję **Zaszyfruj telefon** w polu **Szyfrowanie**.

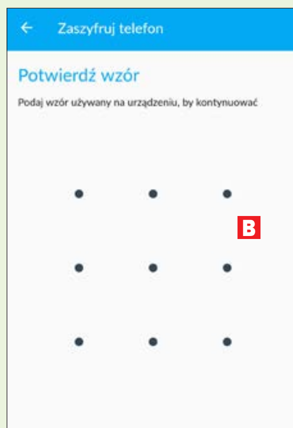
4 Teraz musimy zapoznać się z informacjami dotyczącymi szyfrowania. Jeśli wykonaliśmy wspomniane wcześniej kroki przygotowawcze, będzie dostępna opcja **ZASZYFRUJ TELEFON** **A**, którą wybieramy.

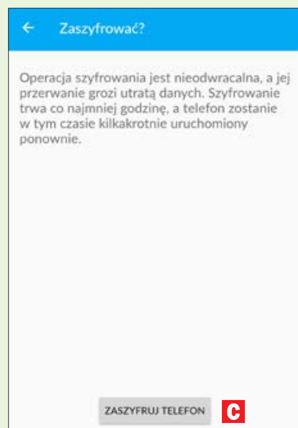
5 Teraz potwierdzamy wzór **B**, hasło lub inną metodę wybraną do zabezpieczania naszego urządzenia.

6 Przechodzimy do ostatniego ekranu, na którym wystarczy nacisnąć **ZASZYFRUJ TELEFON** **C**. **Uwaga!** Operacja jest nieodwracalna i po jej wykonaniu nasze dane zostaną bezpiecznie zaszyfrowane, a dostęp urządzenia będziemy uzyskiwać każdorazowo po jego odblokowaniu za pomocą wzoru, hasła lub innej wybranej przez nas metody.









JAK SKORZYSTAĆ Z E-WYDANIA KSIĄŻKI

W KŚ+ znajdziemy **e-wydanie książki do czytania online i do pobrania w formacie PDF, a także obraz ISO płyty z programami zapewniającymi anonimowość.**

Założ konto Logowanie
Zarejestruj kod

1 Otwieramy stronę **www.ksplus.pl**. Logujemy się ● (używamy konta z serwisu **Komputerswiat.pl**). Jeżeli nie mamy konta, klikamy na ●, by się zarejestrować.

2 Po zalogowaniu się możemy zarejestrować kod nadrukowany na płycie dołączonej do książki. Wystarczy kliknąć na link ● i przepisać kod.

Moje konto
Zarejestruj kod

3 Uzyskamy w ten sposób dostęp do e-wydania ● i do bonusowego obrazu płyty ● zawierającej narzędzia umożliwiające zachowanie anonimowości, w tym te opisane we wskazówkach. Do serwisu KŚ+ możemy logować się zawsze i wszędzie.

CZYTAJ E-WYDANIE
PROGRAMY
BONUSY

UWAGA! W KŚ+ ZA DARMO E-WYDANIE KSIĄŻKI ORAZ PLIK ISO PŁYTY

POLECAMY INNE NASZE KSIĄŻKI, MIĘDZY INNYMI:



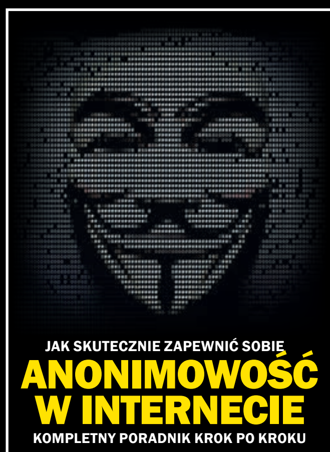
Photoshop: 50 trików

50 praktycznych porad, które pozwolą efektownie poprawić i zmodyfikować zdjęcia lub grafiki oraz fotki w smartfonach



Programuj sam!

Poradnik na start dla przyszłych programistów. Nauczymy się z niego tworzyć gry, aplikacje i pierwsze programy



BĄDŹ ANONIMOWY

Nie możemy całkowicie zniknąć z sieci – potrzebujemy serwisów społecznościowych i innego typu usług. Jednak zawsze należy zadawać sobie pytanie: Czym możemy dzielić się z całym światem, a co ma pozostać naszą tajemnicą?

Z tej książki dowiemy się właśnie, jak skutecznie chronić nasze tajemnice, jednocześnie swobodnie korzystając z internetu.

Poznamy mnóstwo praktycznych programów i trików pokazujących, jak ich używać, by zachować anonimowość i prywatność w sieci.

Nauczymy się między innymi szyfrować dane, dyski i rozmowy, ukrywać IP, posługując się VPN-em i siecią Tor, oraz całkowicie anonimowo korzystać z internetu dzięki systemowi Tails.

Bardzo ważnym elementem książki jest płyta DVD zawierająca bezpieczny system Tails Live DVD i Live USB zapewniający anonimowość oraz zestaw narzędzi do ochrony prywatności w Windows.

CENA 14,90 zł
w tym 5% VAT

Nr 1/2018 (95)





KOMPUTER ŚWIAT BIBLIOTECZKA